

採用における AI ツール

監査結果報告書

2024 年 11 月



内容

エグゼクティブサマリー.....	3
序文	5
主な勧告.....	7
方法論.....	10
インパクト.....	12
所見のまとめ.....	14
データの最小化と目的の制限	14
個人情報 を AI の訓練とテストに利用する	18
AI における正確性、公平性、バイアス軽減	20
透明性.....	25
AI におけるプライバシーのトレードオフ	29
AI におけるヒューマンレビュー.....	31
DPIA とリスクマネジメント	33
情報セキュリティと完全性	36
経営フレームワーク.....	39
サードパーティとの関係	44

エグゼクティブサマリー

ICO は、採用活動で使用される人工知能（AI）搭載のソーシング、スクリーニング、選考ツールの開発者や AI 提供者に対して、同意に基づく監査を行ってきた。我々は、採用プロセスにおける AI ツールの使用が雇用者に利益をもたらす可能性があることを認識しているが、その使用は人々や彼らのプライバシーと情報の権利にとってのリスクにもつながる可能性がある。我々は、AI 採用ツールの開発と提供が英国データ保護法をどのように遵守しているかを理解するため、より広範な AI エコシステムの上流監視の一環として、この作業を実施した。

我々の監査では、AI におけるデータ保護コンプライアンスとプライバシー・リスクのマネジメントに改善すべき点が見つかっただけでなく、優れた実践例も見つかった。我々は、データ保護法の遵守を改善し、我々の公表したガイダンスにあるグッドプラクティスを推進するための行動を勧告した。

多くの AI 提供者が AI ツールの精度とバイアスをモニターし、改善策を講じていた。しかし、精度のテストが不十分な例も見られた。さらに、一部のツールでは、採用担当者が特定の防御的特性を持つ候補者をフィルタリングできるような検索機能があり、識別的差別につながる可能性があった。また、求職者に直接質問するのではなく、応募書類や名前だけから性別、民族性、その他の特性を推定・推測するものもあった。この推測された情報は、バイアスを効果的に監視するのに十分な精度ではない。多くの場合、合法的な根拠なく、候補者が知らないうちに処理されていた。

我々は、必要以上に個人情報を収集するツールを見つけたことに懸念を抱いた。いくつかのケースでは、個人情報がスクレイピングされ、求人ネットワークサイトやソーシャルメディア上の数百万人のプロフィールから他の情報と組み合わせられていた。そして、採用担当者が潜在的な求職者に求人情報を売り込むためのデータベースを構築するために利用された。採用担当者も候補者も、情報がこのように再利用されていることに気づくことはほとんどなかった。

AI 提供者が自らを管理者ではなく処理者と誤って定義し、その後データ保護の原則を遵守していない例がいくつか見つかった。中には、自社のツールを使用する採用担当者にコンプライアンスに関する全責任を転嫁しようとする例もあった。このような場合、通常、曖昧で不明確な契約が結ばれており、意図的に広範な契約を結んでいるように見えたり、採用担当者が何も知らないままだったりする。

しかし、心強い取り組みも数多く見られた。一部の AI 提供者は、採用担当者が自分たちのニーズに合わせてカスタマイズでき、不必要な個人情報の収集を避けることができる、独自のオーダーメイド AI モデルを提供していた。また、可能な限り透明性を確保し、AI とその仕組みに関する詳細な情報をオンラインで共有することで、人々の信頼を築いている AI 提供者もあった。

調査の過程で、我々はコンプライアンスを改善するために約 300 件の勧告を行い、そのすべてが受け入れられた。これらの勧告は、法律に基づく以下のような多くの要件をカバーしていた；

- AI において個人情報を公正に取り扱う；
- 処理を明確に説明する；
- 個人情報の収集は最小限にとどめる；
- 個人情報を違法に再利用または処理しない。
- リスクアセスメントを実施し、プライバシーへの影響を把握する。

AI 提供者も採用担当者も、本報告書の勧告に従うべきである。

高水準のデータ保護コンプライアンスを持つことで、人材採用における AI の開発・利用組織は、イノベーションを起こし、優れたサービスを提供することができ、同時に一般市民との信頼関係を築くことができる。

序文

我々は、採用活動に使用される AI ツールを開発または AI 提供者している組織に対して、同意に基づく監査プログラムを実施した。監査対象となった採用ツールは、ソーシング、選定（スクリーニング）、選考（セレクション）に幅広く使用されている。

ソーシング・ツールは次を含む：

- 候補者プロフィールのデータベースから、採用担当者の求人にマッチする、または最も適した候補者を提案する。
- 性別、民族性、年齢、その他の多様性の特徴を予測または推測して、採用担当者の労働力の多様性を高める可能性のある候補者を見つける。

選考ツールは次を含む：

- 応募書類や履歴書から候補者の能力やスキルを評価する；
- 採用担当者とのやり取りから、求職者の「興味」を予測する。
- 採用担当者の選考プロセスにおいて、候補者が合格する可能性を予測する。

選定ツールは次を含む：

- AI を活用した行動ゲームや心理測定でのパフォーマンスに基づいて、候補者のスキルと職務への適合性を評価する；
- 面接の質問に対する書面での回答と、対面またはビデオ面接のテキスト書き起こしから、候補者の能力とスキルを採点する。
- ビデオ面接で候補者の言葉遣い、口調、内容を評価し、性格タイプを予測する。

この作業は、自然言語処理を含む機械学習など、様々な AI のユースケースをカバーしている。ビデオ面接における感情検知など、生体データの処理に使用される AI は、[生体データと神経技術に関する](#)ガイダンスを検討し、別途作成中であるため、この作業には含めなかった。また、チャットボットや求人広告・職務記述書のドラフトなど、生成的 AI を使用するツールもこの作業には含めなかった。しかし、我々は、採用における生成的 AI モデルの使用が増加していることを認識しており、他の作業において人々のプライバシーに対するリスクを調査している。

我々は、より広範な AI エコシステムの上流への関与と監視の一環として、この作業に取り組んだ。これは、AI 採用ツールの開発、提供、使用におけるプライバシー・リスクと英国データ保護法の潜在的な不遵守を理解するのに役立った。

我々は、AI が効率性、拡張性、一貫性、プロセスの簡素化など、社会に改善をもたらす機会を提供していることを認識している。採用プロセスにおいて AI を使用すれば、組織は潜在的に大量の応募を処理し、一貫性のあるタイムリーな方法で処理することができる。

しかし、個人情報の処理をこのような複雑で時に不透明なシステムに移行することは、人とそのプライバシーに固有のリスクを伴う。人間の採用担当者は、科学的妥当性の確認に限界がある可能性のある AI の出力、スコア、予測に影響を受け、採用決定を下す可能性がある¹。英国政府が『[採用における責任ある AI ガイド](#)』で詳述しているように、AI の採用アルゴリズムは不公平で、人間のバイアスを模倣することを学習し、マイノリティのデジタル排除を永続させる可能性がある²。Centre for Data Ethics and Innovation は 2022 年 12 月の [Industry Temperature Check](#) の中で、膨大な個人情報を保有する AI システムはサイバー攻撃や妨害の標的になりうると指摘している³、特に情報が必要以上に長く保管・保存される場合には注意が必要である。AI は、透明性がなく説明不可能な方法で個人情報を処理したり、妥当性確認やインフォームド・コンセントのない同意に依拠したりする可能性がある。

2021 年 9 月に発表された[国家 AI 戦略](#)に続き、英国政府は 2023 年 3 月に [AI 規制に関する政策文書](#)を発表した。これは、以下の原則に基づき、AI 規制に対してイノベーションを促進するアプローチを導入する計画を定めたものである：

- 安全性、セキュリティ、そして堅牢性だ；
- 適切な透明性と説明可能性を確保する；
- 公正である；
- 説明責任とガバナンス。
- 競争力と救済。

これらの原則は、英国の GDPR におけるデータ保護の原則と密接に関連している。高水準のデータ保護コンプライアンスを持つことで、採用における AI を開発・使用する組織はイノベーションを起こし、優れたサービスを提供することができ、同時に一般市民とのトラストも構築することができる。

¹ REC.REC、AI による英国雇用へのリスクを示す報告書に対応（2024 年 3 月 27 日）

<https://www.rec.uk.com/our-view/news/press-releases/rec-responds-report-showingrisk-uk-jobs-ai>。

² 科学技術革新省、採用におけるガバナンス AI ガイド（2024 年 3 月 25 日）

<https://www.gov.uk/government/publications/responsible-ai-inrecruitment-guide>。

³ データ倫理イノベーションセンター業界温度チェック：

https://assets.publishing.service.gov.uk/media/638f3af78fa8f569f7745ab5/Industry_Te_m_temperature_check_-_Barriers_and_Enablers_to_AI_Assurance.pdf。

主な勧告

我々の監査では、AIにおけるデータ保護コンプライアンスとプライバシー・リスクのマネジメントに改善すべき点がいくつか見つかった。我々は、データ保護法の遵守を改善し、我々の公表したガイダンスにあるグッドプラクティスを推進するための行動を勧告した。

我々の勧告は、AIの使用ケース、処理される個人情報、組織の状況に合わせたものである。しかし、最も一般的な領域を7つの主要な勧告事項にまとめた。これは、AI採用ツールを設計し使用する際に、すべての組織にとって極めて重要なものである。

これらの主要な勧告は、AI採用ツールを開発または提供する組織（AI提供者）と、採用においてAIツールを使用する、または使用を考えている組織（採用担当者）に関連する。

AI提供者と採用担当者は、AIリクルートツールが英国のデータ保護法を遵守するよう、我々の勧告に従うべきである。

推薦の言葉公平性

AI提供者と採用担当者は、AIによる個人情報の公正な処理を保証しなければならない。これには、AIとそのアウトプットに潜在的または実際の公平性、正確性、バイアスの問題がないか監視し、それらに対処するための適切な措置を講じることが含まれる。その結果下される判断や人間の関与の度合いによっては、精度がランダムよりも優れているだけでは、AIが個人情報を公正に処理していることを示すには不十分である。

さらに、**AI提供者と採用担当者は**、バイアスや差別的な出力を監視するために処理される特別カテゴリーデータが、この目的を効果的に果たすのに十分適切かつ正確であることも確認しなければならない。また、この処理がデータ保護法に準拠していることも確認しなければならない。防御データや推定データは、十分かつ正確ではないため、データ保護法に準拠しない。

勧告透明性と説明可能性

採用担当者は、AIによる個人情報の処理方法について、候補者に確実に通知しなければならない。そのためには、詳細な[プライバシー情報](#)を提供するか、あるいはAI提供者から提供されるようにしなければならない。これは明確に説明されるべきである：

- AIがどのような個人情報をどのように処理するか；
- 予測や出力に関わるロジック。
- AIの訓練、テスト、その他の開発のために個人情報をどのように使用するか。

AI提供者は、関連するAIの技術情報やAIロジックの詳細を採用担当者に積極的に提供することで、AIの[透明性と説明可能性](#)をサポートすべきである。

AI 提供者と採用担当者は、候補者にプライバシー情報を提供する責任がどちらにあるのかを契約で明確に定義しなければならない。

勧告データの最小化と目的の限定

AI 提供者は、総合的に以下をアセスメントすべきである：

- AI の各要素を開発、訓練、テスト、運用するために必要な最小限の個人情報を提供する；
- 処理の目的および当初の処理目的との互換性。
- 個人情報を必要とする期間

採用担当者は、以下をすべきである：

- AI の目的を達成するために必要な最小限の個人情報のみを収集する。
- 個人情報を特定の限定された目的のためにのみ処理し、互換性のない別の目的のために保存、共有、再処理しないことを確認する。

勧告データ保護影響アセスメント (DPIA)

AI 提供者と採用担当者は、以下をすべきである：

- 人へのリスクが高い加工が行われる可能性がある場合、AI 開発の初期段階および加工前に [DPIA](#) を実施する。
- AI の発展や処理の変更に応じて DPIA を更新する。

DPIA には、以下を含めなければならない：

- 個人情報処理の結果、人々が被るプライバシーリスクを包括的にアセスメントする；
- これらのリスクを低減するための適切な低減コントロール。
- 人々のプライバシーと他の競合する利益との間のトレードオフの分析。

プロセッサーとしてのみ行動する場合であっても、**AI 提供者は**、プライバシーリスクを評価・軽減し、技術的・組織的管理が実施されていることを証明するために、DPIA の完了を検討すべきである。

勧告データ管理者と処理者の役割

AI 提供者と採用担当者は、以下をすべきである：

- AI 提供者が、個人情報の特定の処理ごとに、[管理者、共同管理者、または処理者のいずれ](#)であるかを定義する。
- このことを契約書やプライバシー情報に明記する。

AI 提供者は、実際に処理の手段と目的を全体的に管理する場合、管理者となる。例えば、採用担当者に代わって処理する個人情報を使用して、すべての採用担当者に展開する中央 AI モデルを開発する場合などである。

勧告する：明示的な処理指示

採用担当者は、処理者として AI 提供者に代わって個人情報を処理する際、AI 提供者が従うべき明示的かつ包括的な書面による[処理指示](#)を定めなければならない。これには、以下の事項を決定することが含まれる：

- 特定のデータフィールドが必要である；
- 処理の手段と目的
- 必要な出力
- 個人情報を保護するための最低限のセーフガード。

採用担当者は、AI 提供者がこれらの指示を遵守し、追加の代替目的のために個人情報を共有または処理していないことを定期的に確認すべきである。

AI 提供者は、人材紹介業者の処理者として個人情報を処理する場合、人材紹介業者の明示的な指示にのみ従わなければならない。AI 提供者は、個人情報を保持したり、許可なく共有したり、指示を超えて独自の目的で処理してはならない。

勧告する：合法的根拠と追加条件

AI 提供者と採用担当者は、以下をすべきである：

- 個人情報を処理する前に、管理者である場合、個人情報処理の各事例において依拠した[合法的根拠](#)を特定すること；
- 特別カテゴリー・データを処理する場合、追加条件を特定する；
- 文書化し、プライバシー情報に記載し、契約書に合法的根拠と条件を記録する；
- 正当な利益に依拠する場合は、正当な利益のアセスメントを完了する。
- 同意に依存する場合は、同意が具体的で、粒度が細かく、明確なオプトインがあり、適切なログが記録され、定期的に更新され、同意の撤回が同意と同様に容易であることを確認する。

方法論

2023年8月から2024年5月にかけて、AIを活用した採用ツールを開発または提供している組織に対して、同意に基づく監査を実施した。

監査の範囲は、以下の主要分野に及んだ：

- **プライバシー管理の枠組み** - AIシステムにおけるプライバシーを支える管理の枠組みを見直す：
 - プライバシーに関する包括的な方針と手順；
 - コンプライアンス・メカニズムとKPI；
 - 主要スタッフに対するプライバシーとAIに関する専門的な研修。
 - 個人情報を処理するための適切な合法的根拠および追加条件を特定**する**。
- **データの最小化と目的の限定** - 個人情報がAIの開発や提供に再利用されないようにし、処理される個人情報は必要最小限かつ適切で、必要以上に長く保持されないようにする。
- **サードパーティとの関係** - AI提供者と採用担当者が、管理者責任と処理者責任を理解し、履行していることを確認し、契約においてこれらを正式なものとする。
- **情報セキュリティと完全性** - 技術的なセキュリティ対策とアクセス管理が実施され、収集時、輸送時、保管時に個人情報が効果的に保護されていることを確認する。
- **透明性** - AI採用ツールにおいて個人情報がどのように処理されるかを人々に確実に知らせる。
- **DPIA およびリスクマネジメント** - データ保護影響アセスメント（DPIA）が完了し、人々に対するプライバシーリスクの包括的なアセスメント、およびこれらのリスクを低減するための効果的な低減策が含まれていることを確認すること。
- **AIにおけるプライバシーのトレードオフ** - AIシステムにおいて、人々のプライバシーとその他の競合する価値や利益との間で起こりうるトレードオフが、慎重に評価され、回避されていることを確認する。
- **AIの訓練とテストに個人情報を利用する** - AI開発のために個人情報がどのように公正かつ透明性をもって利用されてきたかを検証する。
- **AIにおけるアセスメント、フェアネス、バイアスの低減** - AI開発において、フェアネス、アセスメント、バイアスの問題がどのように低減され、AIのライフサイクルを通じて効果的に監視されているかを評価する。
- **AIにおける人間によるレビュー** - AI、その処理、およびそのアウトプットが、有意義な人間によるチェックと正式なレビューの対象となり、問題がタイムリーに対処されるようにする。

監査は、当局のデータ保護監査手法に従って実施された。その主な要素は以下の通りである：

- 関連する方針および手順を机上でレビューする；
- 主要なプライバシー・コンプライアンスおよび AI 技術スタッフへのインタビュー。
- AI 設計書、システム仕様書、管理情報を含む証拠書類のレビューを行う。

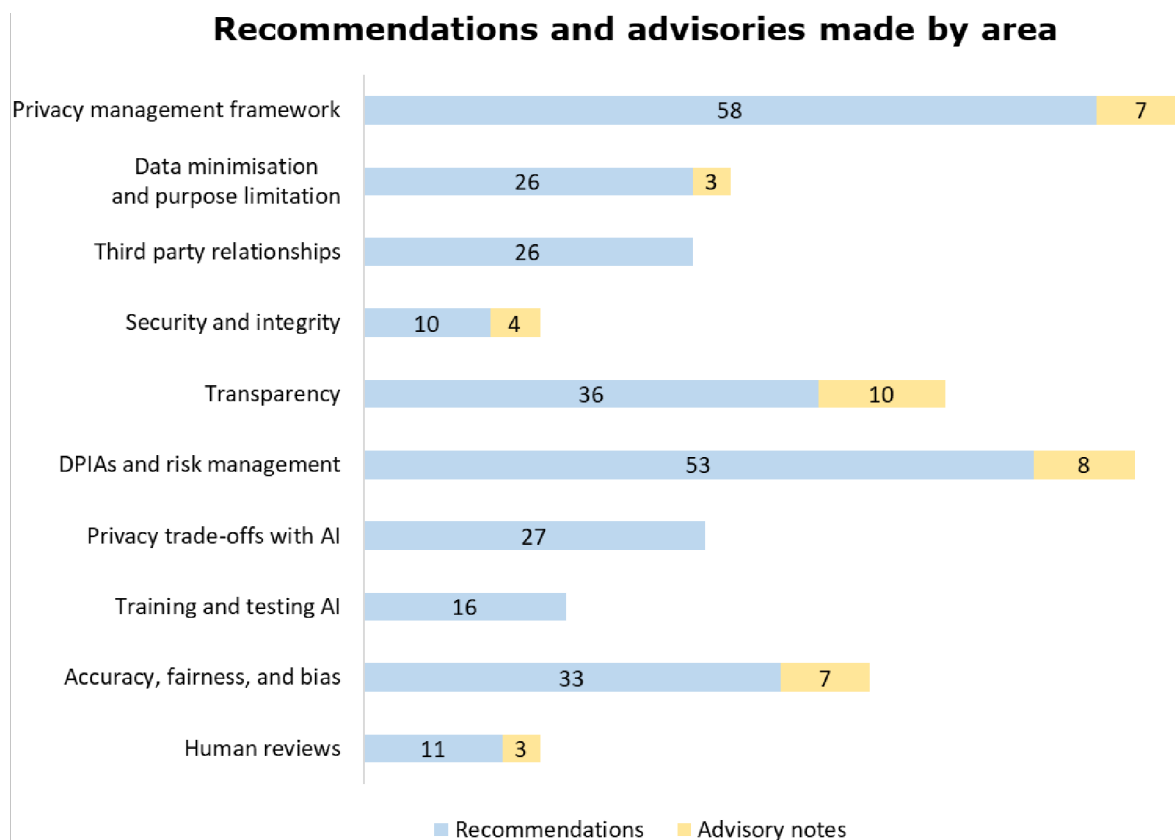
各組織について同じ重点分野を検討し、主要なテーマを特定できるようにした。

我々の作業から得られた知見は、「スナップショット・イン・タイム」としてとらえたものであり、各エンゲージメントの時点で我々が発見した内容に基づいている。組織はその後、コンプライアンスを改善し、リスクを軽減するための措置を講じている可能性がある。

各組織は個別に監査報告書を受け取った。弱点や機会を特定した場合には、データ保護法の遵守を改善し、既存のプロセスを強化するための勧告を行った。

インパクト

ICO の監査人は、全業務を通じて 296 件の勧告と 42 件のアドバイザリーノートを行った。分野別の内訳は以下の通りである：



最初の監査関与の後、我々はすべての組織に対し、我々の勧告に適切な対応をとるよう要請した。各組織は積極的に対応し、以下のように自主的にコンプライアンス改善のための迅速な行動を取ることを厭わなかった：

- 勧告の **97%** が受け入れられ、アクションが設定された。
- 勧告の **3%** が部分的に受け入れられ、アクションが設定された。
- 却下された勧告はなかった。

また、監査の経験や組織への付加価値についても意見を求めた。対応は以下のように 10 点満点で採点した：

- **9.3** : 英国データ保護法の要求事項の理解を改善する。
- **9.7** : AI ツールにおける主要なプライバシーリスクについての理解を改善するためのものである。
- **9.0** : AI ツールにおけるプライバシーリスクの低減を支援している。
- **9.3** : シニアリーダーとの情報プライバシーに関する意識の向上を支援する。

また、各団体は我々との関わりについて、以下のようなコメントを寄せている：

「プロセスは簡単で効率的だ。

「よく管理されており、非常にプロフェッショナルだった。

「とても役に立ち、勇気づけられた。

「監査は、コントローラとプロセッサーとの関係をめぐるわれわれの位置づけのいくつかを確認し、われわれ自身の考えや研究を促した。

「監査は、DPIA とそのギャップについて検討するきっかけとなった。

最後に、初回監査の後、重大な未解決のリスクやコンプライアンス違反の領域がある特定の組織について、フォローアップを行った。我々は、これらの重要なリスク分野の進捗状況と裏付けとなる証拠を確認し、これらの組織が我々が行った勧告の実施に向けて取り組んでいることを確認した。

所見のまとめ

以下の調査結果は、我々の監査プログラム中に見られた主な指摘事項、改善の機会、優れた事例をまとめたものである。

データの最小化と目的制限

AI システムの開発には一般的に、AI モデルを訓練して確実にタスクを再現したり、アウトプットを生成したりするために、大量の個人情報が必要となる。これらはデータ保護の原則、特にデータの最小化と目的の限定に抵触する可能性がある。我々はこれを見直した：

- どのような個人情報を処理していたのか；
- それが必要なものに限定されているかどうか。
- 必要な期間だけ保管し、他の不適合な用途に再利用しなかったかどうか。

これは、英国 GDPR 第 5 条(1)(a)～(e)を遵守するためである。

大半の AI 提供者は、AI ツール開発のアプローチにおいて、データの最小化を考慮していた。一般的に、AI 提供者は人々から収集する情報を以下のように限定している：

- その人の名前だ；
- 連絡先
- キャリアの経験がある；
- 関連スキル
- 関連する資格または認定。

多くの AI 提供者は、採用担当者の指示があれば、追加情報も処理する。

考慮事項： AI を活用したゲームやアセスメントツールは、可能な限り候補者の名前とメールアドレスのみを収集するように設計する。

事例： 一般的なジョブ・ネットワーキング・サイトから潜在的な候補者のプロフィールのデータベースを管理している AI 提供者は、一般的に、その人の名前、連絡先情報、キャリア経験、関連スキル、関連する資格や認定のみを収集し、保存している。

また、少数ではあるが、本人の写真など、それほど重要でない情報も収集・保存していた。我々は、これらの AI 提供者に対し、各 AI 要素の運用に最低限必要な個人情報を評価するよう勧告した。

ほとんどの AI 提供者は、AI ツールを効果的に運用するために必要な最低限の個人情報をアセスメントしていた。特に、発売前の AI の訓練やテスト、発売後のメンテナンスに必要な情報であ

る。その中には、DPIA やポリシーに最低限のデータ・プロファイルを記録し、各データ・ワールドが必須か否かの理由を明確に正当化しているところもあった。

考慮事項：可能であれば、仮名化された個人情報のみ、または集約された情報のみを使用して AI を開発する。これにより、個人が特定されたり、AI が無関係な情報から学習したりするリスクを最小限に抑えることができる。

考慮事項：最小化されたデータセットと k-fold クロスバリデーションなどのテクニックを使用して、AI ツールの訓練とテストを行う。これにより、データセットを何度も使用することができ、大量の情報を必要とせず精度を向上させることができる。

大半の AI 提供者は、AI ツールの訓練、テスト、保守のために、システム内の候補者の個人情報を再利用していた。いくつかのケースでは、候補者のプロフィールを仮名化または匿名化することで、他の製品の開発にも利用していた。多くの場合、AI 提供者は、このような候補者の個人情報の二次利用が、もともと情報を収集した際の処理目的に適合していることを証明できなかった。

考慮事項：個人情報が効果的に匿名化されていることを確認し、その処理が英国データ保護法の対象外となるようにする。識別や仮名化された情報は、依然として英国のデータ保護法の対象者である。

事例：潜在的な候補者のプロフィールのデータベースを管理する AI 提供者は、通常、求人ネットワークサイトやソーシャルメディア、その他のオープンソースのウェブコンテンツの公開プロフィールから、この情報を大量に収集している。このように大量の情報をスクレイピングしたり、データベンダーからスクレイピングされた情報を購入する場合、すべての AI 提供者がそうではない：

- 情報の新たな利用が当初の処理目的と両立することを証明できる。
- 就職情報サイトやソーシャルメディアサイトからは、情報が合法的に収集され、プライバシーリスクや潜在的な損害から保護されていることを確認する契約書や同意書が必ず提出されていた。

AI 提供者は、収集された当初の目的および合法的根拠と相容れない新たな目的および合法的根拠のために個人情報を処理しないよう勧告した。また、このような取り決めを契約書や合意書に文書化することを勧告した。

考慮事項：情報サプライチェーン全体を通して目的の適合性をアセスメントし、これを契約、デューデリジェンス、データベンダーとの継続的な保証チェックに組み込み、目的制限原則を遵守する。

ほとんどの AI 提供者は、候補者情報の保存期間を採用担当者に依存していた。これは通常、求人募集が終了してから 1 年か 2 年で、契約書に明記されていることが多かった。また一般規定

には、AI 提供者が処理を停止し、情報を採用担当者に送り返すまでの時間を確保するため、契約終了後も短期間は候補者情報を保持するという条項が含まれていた。

考慮事項：自動保持メカニズムが、期待通りに保持期間終了時に個人情報を削除していることを確認する。

事例：候補者プロフィールの大規模なデータベースを管理しているいくつかの AI 提供者は、個人情報をデータベースに無期限に保持する意向を記録していた。彼らは、その情報を定期的に「除草」して、古くなったり、不正確であったり、もはや必要でない可能性のある情報を削除していなかった。必要以上に、あるいは無期限に情報を保持することは、英国 GDPR のデータ最小化および保存制限の原則に準拠する可能性は低い。

個人情報は、意図した処理目的を果たすために必要な期間のみ保持され、保持期間は明確かつ透明性をもって記録されることを勧告した。

考慮事項：不要になった個人情報、不正確である可能性の高い個人情報、古くなった個人情報を「除草」または削除する機会を探す。

AI 提供者への勧告は以下の通りである：

- AI の各要素を操作するために必要な最小限の個人情報をアセスメントし、より少ない個人情報または全く個人情報を使用せずに、同じまたは類似の結果を達成する代替案を検討する。
- 処理されるすべての個人情報が、意図された目的を果たすために明らかに適切かつ正確であることを確実にする。
- データ・ミニマム化、目的制限、その他のデータ保護の原則に対するアプローチを、関連するポリシーや AI 開発文書に文書化し、プロ・プライバシー文化を促進する。
- 収集された当初の目的および合法的根拠と相容れない新たな目的および合法的根拠のために個人情報を処理しない。これには、保持されている情報、および公共の求人ネットワークサイト、データベンダー、人材紹介会社などのサードパーティから入手した情報が含まれる。
- 個人情報は、意図した処理目的を果たすために必要な期間だけ保持し、契約書やプライバシー情報に保持期間を記録する。個人情報を無期限に、あるいは将来有用になる場合に備えて保持しない。

採用担当者への勧告は以下の通りである：

- AI ツールによって収集された個人情報を確認し、これが処理の目的を果たすために必要な最小限のものであることを確実にする。
- 個人情報が、当初の目的および合法的根拠と相容れない、新たな目的および別の合法的根拠の下で AI 提供者によって処理されていないことを確認する。

- 契約書、プライバシー情報、保管スケジュールにおいて、保管期間を一貫して詳細に記録する。これには、AI 提供者が各カテゴリーの個人情報を保管する期間とその理由、保管期間の終了時にどのような措置を取るかなどが含まれる。

□ **良い実務例**：ある AI 提供者は、採用担当者に対し、候補者の応募書類の各要素について指標となる評点を与えていた。彼らは AI ツールにデータ最小化のアプローチを組み込み、AI を運用するために必要な最小限の個人情報を総合的に評価した。その結果、職歴は 10 年までしか収集しないなどの決定を下した。彼らはまた、AI の設計に目的制限を組み込んだ：

- 各採用担当者に、その採用担当者の候補者情報のみを使用して訓練されテストされた AI ツールの別バージョンを AI 提供者として提供する。
- 任意で、AI ツールのバイアスを監視する目的で、候補者の人口統計情報を候補者から直接収集する。

ケーススタディ組織 A は、候補者の大規模なデータベースを構築するために、一般の求人ネットワークサイトやデータベンダーから候補者のプロフィールを入手した。AI 検索ツールを使って、採用担当者の求人に関連するスキルや経験を持つ候補者を特定した。同社が公表したプライバシー情報には、データベース内の候補者プロフィールは 1 年間保持されると記載されていた。しかし、プロフィールが新しい情報に更新されるたびに保存期間が再開されるため、実際にはデータベースの大半が無期限に保存されていた。データベンダーから大量に個人データを調達する際、その情報がどこから調達されたものかを確認したり、本来の収集目的と相容れない新たな目的のために処理していないかどうかを検討したりしていなかった。

我々は、組織に対し、保存期間とその適用方法を見直し、定期的に保存期間を再開することで、情報を無期限に保持しないよう勧告した。また、データベンダーから情報を大量に調達する際には、情報の目的適合性を慎重にアセスメントし、情報が違法に再利用されないようにすることを勧告した。

採用担当者は、類似のサービスを利用する際にも目的の適合性をアセスメントし、候補者を特定するためにこれらのサービスを利用する際にも情報を再利用していないことを確認する必要がある。

詳細：

- 目的の制限 - 原則(b)
- データの最小化 - 原則(c)
- 保管制限 - 原則(e)
- データ最小化の原則について、我々はどのような配慮が必要だろうか。しなければならないか？

個人情報を用いた AI の訓練とテストに利用する

英国 GDPR 第 5 条(1)(a)および(b)、ならびに第 5 条(2)を遵守するため、質の高い代表的なデータセットを用いて AI が適切に訓練され、一貫した信頼性の高い出力が得られるよう、別のデータセットを用いてテストされているかどうかを検証した。

ほとんどの AI 提供者は、単一の AI モデルを開発し、全採用担当者の情報を使って一元的に訓練・テストした後、同じ方法で全採用担当者に展開していた。AI 提供者は、採点や評価アルゴリズムの変更など、AI への変更を採用担当者に展開する前にテストしていた。

ほぼすべての AI 提供者は、採用担当者から収集した候補者情報を使って、ツールの訓練やテストを行っていた。彼らは通常、AI の訓練やテストに使用する前に、情報を仮名化、非特定化、匿名化していた。

考慮事項：複数の採用担当者から得た個人情報を使用して、独自の AI ツールや製品を訓練、テスト、またはその他の方法で開発する場合、管理者は貴社となる。これは、貴社がこの処理の手段と目的を実際に管理する可能性が高いためである。

考慮事項：個人情報を使用せずにベースとなる AI モデルを開発し、各採用担当者の候補者のみを使用して、AI ツールを個別に訓練およびテストする。こうすることで、AI を採用担当者ごとにカスタマイズすることもできる。

考慮事項：k-フォールド交差検証を使用して AI ツールを訓練し、テストする。これにより、最小化されたデータセットを使用して、AI の訓練とテストを複数回行うことができる。

AI 提供者は通常、訓練データとテストデータを分離し、訓練に使用したのと同じ情報で AI をテストしないようにしていた。データのラベル付け、「訓練」または「テスト」のキーの割り当て、別々のデータベースへの情報の格納など、明確な分離を確実にするためにさまざまなテクニックを使用していた。

ほとんどの AI 提供者は、訓練データとテストデータの不均衡による AI のバイアスリスクを認識していた。しかし、データセットが多様で、関連する母集団を代表するものであることを保証するために、すべての業者がサンプリング技術を使用していたわけではない。他の AI 提供者は、データセットから人口統計情報やプロキシを「クリーニング」することでバイアスを軽減しようとしているか、軽減せずにバイアスのリスクを受け入れていた。

AI 提供者への勧告は以下の通りである：

- データラベルとデータラベリングプロセスが明確で、特に「エッジケース」や異常な状況において正確に適用されていることを確実にする。

- AI 開発の次の段階に進むために満たさなければならない特定の規準や目標を含め、AI ツールの訓練とテストのプロセスを文書化する。これにより、AI の訓練とテストに一貫したアプローチが確保される。
- 訓練や AI テストのために個人情報を使用する場合は、その旨を明確に伝える。これには、この目的のために個人情報を処理するために依拠する法的根拠も含まれる。
- 必要なくなったら、訓練・データセットとテスト・データセットを削除する。
- AI の訓練とテストに使用する情報の人口統計学的特性を監視する。データセットが母集団や異なるグループの人々の代表者であることを保証するために、特性やグループの代表の過不足などの不均衡を最小限に抑える。

採用担当者への勧告は以下の通りである：

- AI 提供者に以下の保証を求めるか、証拠を入手する：
 - AI ツールの訓練およびテストに使用される情報の人口統計学的特性を監視する。
 - 訓練データセットとテストデータセットにおいて、ある特性やグループの代表の過不足などの不均衡を識別し、最小化している。
- AI 提供者が、AI ツールや製品の訓練、テスト、開発のためにあなたの候補者の個人情報を使用しているかどうかを明確にすること。AI 提供者が、あなたの情報を使って、あなたの使用のためだけに特注の AI ツールやアルゴリズムを訓練し、あなたの明示的な指示に基づいて行動している場合、その AI 提供者はプロセッサである可能性がある。AI 提供者が、あなたの情報を使って中央の AI ツールまたはアルゴリズムを訓練し、その AI ツールまたはアルゴリズムが採用担当者の全員または数名によって使用される場合、AI 提供者はその処理の管理者となる。

□ **良い実務例**：ある AI 提供者は、候補者のスキルや行動を予測するためにゲームベースのアクセスメントを行っている。アクセスメント後に任意でアンケートを実施し、受験者から直接人口統計学的特徴を収集し、匿名プロフィールに追加した。これを利用して、訓練データとテストデータセットが関連する母集団の代表者であることを確認した。受験者から人口統計学的情報が提供されなかった場合、AI 提供者は匿名化されたプロフィールを第 3 のデータセットに追加した。これは、最初の訓練とテストの後、精度とバイアスの指標を比較するためのデータセットで、ツールの妥当性を再度確認するために使用された。

ケーススタディ：組織 A は、候補者の大規模なデータベースを構築するために、一般の求人ネットワークサイトやデータベンダーから候補者のプロフィールを入手した。AI 検索ツールを使って、採用担当者の求人に関連するスキルや経験を持つ候補者を特定した。彼らは、データベース全体を訓練、テスト、妥当性確認に分けようとしていた。しかし、実際にこれらをどのように分けているのかは明確ではなかった。AI が情報を使って訓練され、同じ情報を使ってテストされる場合、精度やバイアスの問題が検出されず、「本番稼働」前に対処されない可能性が

ある。また、訓練、テスト、妥当性確認の間で情報をランダムに分割していたため、データセットが代表者であることを保証していなかった。

我々は、AI が訓練されたのと同じ情報でテストするのを避けるため、訓練データとテストデータを別々に保管することを勧告した。また、テストとテストを始める前に、テストと訓練のデータセットが人口統計を代表するものであることを確認し、不均衡を最小化することを勧告した。

採用担当者は、AI ツールを使用する前に、代表的なデータセットで AI ツールが訓練されテストされていることの保証を求めるか、証拠を入手すべきである。

詳細：

- [AI の開発とその目的をどのように区別すべきか？展開するのか？](#)

AI における正確性、公平性、バイアス低減

公正さは、AI の設計と開発全体を通じて重要な考慮事項でなければならない。我々は、英国 GDPR 第 5 条(1)(a)から(e)および第 25 条を遵守するために、AI の AI 提供者が定期的に正確性とバイアスを監視し、AI のライフサイクルを通じて問題に迅速に対処しているかどうかをアセスメントした。

AI 提供者は通常、開発中に AI ツールの精度を考慮し、発売前にアセスメントを行って、それが確実に正確な出力を生成することをテストしていた。彼らは、AI と期待される結果との間に正の相関関係があるかどうかをテストするために、精度、再現率、曲線下面積、その他同様の測定基準を組み合わせて精度を測定していた。

事例： AI 提供者は AI ツールを開発する際、精度の許容範囲や最低目標を独自に設定する傾向があった。ある AI 提供者は、ほぼ完璧な正の相関を示すデータポイントのみを AI ツールに組み込んでいた。また、わずかな正の相関を示すデータポイントまで、より幅広いデータポイントを受け入れ、ツールの指示的な性質に依存している AI 提供者もあった。AI 提供者は通常、ツールの全体的な精度を改善するために、正の相関がないデータポイントを除外したり、重み付けを減らしたりするプロセスを持っていた。

大半の AI 提供者は、発売後、特に変更やアップデートを実施する前に、少なくとも定期的に精度テストを繰り返していた。これにより、精度が許容範囲内に保たれ、時間の経過とともに低下することがなかった。

事例： ある AI 提供者は、発売前に計画的なテスト手法を使って AI ツールの精度を正式に評価していなかった。その代わりに、自社の AI ツールが「少なくともランダムよりは優れている」ことを頼りにしていた。

この場合、AI は非常に限定された分野でのみ指標となる評点を出し、採用担当マネージャーをサポートするためだけに設計されていた。また、採用担当マネージャーは、成績はあくまで目安であると明記された研修や資料を受け取っていた。採用担当者は不正確な成績を変更し、AI はそれを訓練して時間の経過とともに精度を向上させた。

しかし、AI が人間の介入なしに積極的に採用決定を行うような場合、「少なくともランダムよりはまし」であるだけでは、データ保護法を遵守するには不十分である。このような場合、AI 提供者は立ち上げ前に AI の精度をアセスメントし、監視し、精度の問題に対処することを勧告する。AI は、個人情報処理する前に、目標とする精度レベルに達するべきである。

採用担当者は、AI ツールを使用する前に、それをどのように使用するつもりなのか、また、その決定が採用プロセスにおいてどのような影響力を持つのかに基づいて、AI の精度が十分かどうかを検討することをお勧めする。採用担当者は、不正確な AI だけに頼って判断を下すべきではない。

考慮事項： ツールを起動する前に、すべてのデータポイントの妥当性と正確性を確認する。テストなしでさらにデータポイントを作成することを制限する。これにより、起動後の精度低下を防ぐことができる。

考慮事項： 認知行動学や心理測定の専門家を活用し、AI のロジック、スコアリング、出力に正確性やバイアスの問題がないか定期的にテストし、レビューする。

AI 提供者は、通常、悪影響分析手法を用いて潜在的なバイアスを測定することで、AI ツールにおけるバイアスの可能性も考慮していた。多くの場合、最低基準値として「5 分の 4 ルール」を用いている。これは、どのグループの選択率も、最も選択率の高いグループの選択率の少なくとも 5 分の 4、つまり 80% 以上でなければならないことを意味する。

AI 提供者は一般的に、バイアスが確認された AI ツールを改善するためにとった行動を示すことができた。例えば、データポイントの重み付けを減らす、バイアスに悪影響を及ぼすと思われるデータポイントを除外する、グループに悪影響を及ぼすと思われるデータポイントを除外する、などである。通常、少なくとも定期的に、あるいは AI ツールの変更を開始する前に、バイアステストを繰り返している。

事例： いくつかの AI 提供者は、個人情報を直接収集するのではなく、個人情報や候補者プロフィールの他の部分から、その人の特性を推定または推測することを選択した。これは通常、その人の性別や民族性を予測するもので、多くの場合は名前からだが、時には候補者のプロフィールや応募書類の要素から予測することもある。彼らはこれを、その人についてすでに持っている情報に加えた。

このようにして意図的に推測された情報は、依然として特別なカテゴリーデータである。AI 提供者は、推論された情報を常に特別なカテゴリー・データとして扱ったり、処理の追加条件を

特定したりしてはいたわけではない。合法的な根拠と追加条件なしに特別カテゴリーデータを処理することは、英国の GDPR では合法的である可能性は低い。このような方法で追加の個人情報を作成することは、しばしば目に見えず、透明性がなかった。これは、受験者がこのようなことが起こっていることを必ずしも明確に知らされておらず、作成された追加情報にアクセスできないためである。

我々は、これらの AI 提供者に対し、特殊カテゴリーデータを処理する前に、合法的根拠と追加条件を特定し、正確な情報を合法的に収集する代わりに、推測される情報を使用しないよう勧告した。

AI ツールのバイアスを測定、監視、対処するために、推測または推定された情報を使用することには、いくつかの限界があった。バイアスのモニタリングは、性別、民族性、年齢のみに限定されていた。利用可能な情報から、英国平等法 2010 の他の防御特性を推定することはできなかった。性別、民族性、年齢を正確に推定できるのは、例えば「男性」や「女性」、民族性では「白人」、「黒人」、「アジア系」といった大きなカテゴリーに限られていた。これより小さなカテゴリーでは信頼性の高い推定は困難であり、効果的に測定するにはサンプルが少なすぎる可能性が高い。

推論された情報を使用する AI 提供者は一般的に、AI ツールにおいてバイアスを効果的に低減するのに十分な信頼性と正確性を実証することができなかった。つまり、AI ツールにバイアスが忍び込んでも、バイアステストではそれが浮き彫りにならないリスクが大きい。このリスクを適切にアセスメントしている AI 提供者はほとんどなかった。

考慮事項：合格者から収集した人口統計学的情報を新入社員の平等モニタリングに再利用することで、人口統計学的情報を推測するよりも正確なバイアスを測定することができる。ただし、この方法で情報を再利用することは、英国 GDPR の目的制限原則に準拠する可能性は低く、この目的には適切な合法的根拠が必要となる。

考慮事項：採用プロセス後に任意でアンケートを実施し、候補者から直接人口統計学的情報を収集する。AI 提供者が提供されている場合はより正確にバイアスをモニターするために、提供されていない場合は未知のサンプルを使って追加の妥当性確認テストに利用できる。

AI 提供者が悪影響分析の手法を使って潜在的なバイアスを測定しなかった場合、通常、AI が入力情報の個人的特徴について盲検化することに頼っていた。これは、入力情報から人口統計学的情報やプロキシを削除することによって行われた。

考慮事項：AI がビデオインタビューの録画を処理する際にバイアスがかかっていないか監視し、人口統計学的特徴のプロキシを削除したり、AI の訓練プロセスやモデルを修正することでバイアスを軽減する。

考慮事項：悪影響のassessmentやAIのソースコードに誤りがないかのレビューなど、AIツールの外部監査を実施する。

考慮事項：国家プロジェクト、業界連携グループ、利害関係者ネットワークと定期的に連携し、AIの開発・提供における新しいアイデアを開発し、優れた事例を共有する。

AI 提供者への勧告は以下の通りである：

- AIが公正に運営され、マイノリティグループを識別的に差別していないことを、以下の方法で証明する：
 - AIツールやアウトプットの公正さ、正確さ、バイアスの問題を定期的にテストする；
 - 識別した問題に効果的に対処する；
 - 主要業績評価指標の正確性とバイアスを、上級管理職および主要利害関係者に定期的に報告する。
 - テスト結果や報告書、および問題に対処するためにとった措置の証拠を保持すること。
- AIツールにおける潜在的または実際の公平性、正確性、バイアスリスクをassessmentし、軽減する：
 - AI開発には人間のバイアスが存在する；
 - 訓練情報とテスト情報のサンプリングバイアス；
 - 不適切または不十分な情報表示。
 - 人口統計学的情報をテキストまたはビデオで提示する。
- 公平性とバイアスを監視する際には、以下のような幅広い特性を考慮する：
 - ジェンダーとジェンダー・アイデンティティである；
 - 人種または民族的出身、身体障害、および
 - 英国GDPRのリサイタル71に記載されているその他の特性、または英国平等法2010の保護特性。
- アルゴリズムによる公平性の制限を評価し、それをどのように回避するか考慮事項：
 - 保護された特性が不平等に分布している；
 - 複数の保護特性を持つ人々。
 - 訓練データとテストデータに存在する保護特性のプロキシ。

- AI のアウトプット、特に不公平、不正確、またはバイアスのかかったアウトプットに関する苦情に異議を唱える候補者に対して、スタッフがどのように記録し、対応すべきかを文書化する。

採用担当者への勧告は以下の通りである：

- AI 提供者が、AI ツールの公平性、正確性、バイアスをどのように監視し、低減しているか、特にそのためにどのような個人情報を使用しているか、またその情報源はどこかを確認する。
- 個人情報の処理または AI ツールの運用における、潜在的または実際の公正性、正確性、バイアスリスクと、それらを軽減するための措置を検討する。これらのリスクを DPIA に記録する。
- AI のツールや出力における公平性、正確性、またはバイアスの問題に対処するために AI 提供者がとった措置について、テスト結果や報告書、証拠を求める。これらが、AI が公正に運用され、マイノリティ・グループを識別的でないことを実証していることを確認する。

□ **良い実務例**：一部の AI 提供者は、ゲームベースのアセスメントを行い、候補者のスキルや行動を予測していた。彼らはツール開発の各段階で精度とバイアスのアセスメントを組み込んでいた。彼らはツールの発売前に各データポイントの正確性と妥当性を確認し、各データポイントについて人口統計グループごとのバイアスと悪影響を測定した。発売後も定期的のアセスメントを繰り返した。ツールのアウトプットは、認知行動学と心理測定学の専門家チームによって監督され、各募集キャンペーン後に人口統計学的グループごとのスコア分布を比較した。

ケーススタディ：組織 A は、候補者の大規模なデータベースを構築するために、一般の求人ネットワークサイトやデータベンダーから候補者のプロフィールを入手した。AI 検索ツールを使って、採用担当者の求人に関連するスキルや経験を持つ候補者を特定した。彼らは検索ツールの精度をテストしたが、社内でバイアスのテストは行っていなかった。その代わりに、この目的のために作られた人工的なデータセットのみを使用して悪影響をテストする外部組織を使用した。彼らは候補者の名前とその他のプロフィール情報から性別と民族を推測した。しかし、バイアスの低減ではなく、採用担当者が候補者リストから属性をフィルタリングできるようにするためにこれを使用した。

我々は、組織がバイアスと識別の可能性をテスト・監視し、そのために正確で適切な情報を効果的に使用することを勧告した。また、AI とその処理における公平性、正確性、バイアスのリスクを評価し、軽減するよう勧告した。

採用担当者は、AI を使用する前に、また使用後も定期的に、テスト結果や問題が解決された証拠を確認することで、AI が公正に運用され、マイノリティ・グループを識別的に差別していないことをチェックすべきである。

詳細：

- [正確さと統計的正確さについて何を知る必要があるのか？](#)
- [公平性、バイアス、差別はどうなのか？](#)
- [ML モデルにおける識別的低減のための技術的アプローチとは何か？](#)
- [AI を使って推論する](#)
- [AI のライフサイクルにおける公平性](#)
- [グッドワーク・アルゴリズム・インパクト・アセスメント \(IFOW\)](#)

透明性

AI の開発者と導入事業者は、AI を使ってどのように個人情報を処理し、採用の決定やアウトプットを出すかについて、オープンで透明性があることが重要である。我々は、英国 GDPR 第 5 条(1)(a)、第 13 条、第 14 条に準拠するため、人々が理解できる明確で非技術的な説明が積極的に提供されたことを確認した。

AI 提供者は、プライバシー情報をウェブサイト上のプライバシーポリシーで公表していた。プライバシーポリシーはテキストベースで、小見出しのあるセクションで構成されていた。我々がレビューしたほとんどのプライバシーポリシーには、少なくとも以下の項目が含まれていた：

- 処理した個人情報分野の概要；
- 処理の主な目的である；
- 情報保護のための保護措置；
- 英国の GDPR における人々の権利、および
- AI 提供者および監督当局の連絡先。

事例：いくつかの AI 提供者は、1 つのプライバシーポリシーで、複数の異なる個人情報処理の事例、複数の異なるカテゴリの人々、あるいは複数の異なる管轄区域や法律をカバーしていた。ほとんどの場合、これは誤解を招き、人々を混乱させる可能性があった。

我々は、これらの AI 提供者が、人々に適切な情報を提供する明確なプライバシー情報を作成することを勧告した。例えば、プライバシー情報を活動ごとに明確なセクションで構成したり、各処理や人々のカテゴリに合わせたプライバシー情報を作成したりする。

考慮事項：自社の AI プラットフォーム上で候補者専用のプライバシーポリシーを作成し、英国の GDPR 要件に関連させる。これにより、受験者はどの情報が自分に関連するのかを理解し、正しく通知される。

考慮事項：テキスト・ベースのプライバシー情報を、情報量の多いポップアップ・メッセージや、処理が行われる時点での一口サイズの情報、あるいはデータ・フロー・マップのような視覚的な資料で補足する。

いくつかのプライバシーポリシーには十分な詳細が含まれていなかった：

- 各個人情報処理の具体的な事例を示す；
- 具体的に依拠した合法的根拠と追加条件、あるいは
- その情報をどれくらいの期間保持するだろうか。

プライバシーポリシーの中には、AI 提供者が管理者なのか処理者なのかが明記されていなかったり、間違っていたりするものもあった。

考慮事項：特に情報処理や AI 機能の変更を実施する前に、プライバシー情報やリソースが正確であることを定期的を確認する。

事例：AI 提供者が二次的または代替的な目的で個人情報を処理する場合、必ずしもプライバシー・ポリシーにその旨が記載されていなかった。例えば、バイアスを軽減するために人口統計学的情報を推測したり、AI の訓練およびテストに使用したりする場合、受験者はこのような処理が行われていることに気づかなかった。

AI 提供者は、自分の情報がどのように処理されるかを、透明性をもって十分に知らせることを勧告した。透明性のない個人情報処理は、英国 GDPR 第 5 条(1)a において合法的であるとは考えにくい。

考慮事項：モデル・プライバシー情報や、技術的な AI 処理をわかりやすく説明した文章を AI 提供者に提供する。これにより、採用担当者は AI システムを理解し、候補者に正確に伝えることができる。

考慮事項：あなたが自分の情報をどのように処理しているかを、人々が実際に理解しているかどうかを確認する：

- プライバシー情報をユーザーとテストする；
- フォーカス・グループや調査を実施する。
- 候補者がプライバシー情報を開いたときのトラッキングを行う。

我々がレビューしたいいくつかのプライバシーポリシーは、AI について非常に大まかにしか言及していない。個人情報や AI ツールの中でどのように処理されるのか、例えば予測や出力に関するロジックや、個人情報が AI の訓練やテストにどのように使われるのか、具体的に知らされていないければ、処理は事実上見えない。

考慮事項：情報やリソースを積極的に公開し、過度に複雑な説明や技術的・法律的な表現を避ける。そうすることで、AI 製品への信頼を築くことができる。

我々は、AI 提供者と採用担当者が、どちらの当事者が求職者の個人情報をどのように処理しているかを知らせる責任があるかを明確に定めた契約を結ぶことを期待した。ほとんどの AI 提供者は、個人情報の取り扱い方法を候補者に通知する管理者として、採用担当者に依存していた。しかし、AI 提供者と採用担当者間の契約では、どちらの当事者が候補者への通知やプライバシー情報の提供に責任を負うのかが不明確であることが多かった。

AI 提供者への勧告は以下の通りである：

- 個人情報の管理者または契約上の AI 提供者である場合は、個人情報をどのように処理しているかを知らせるために、詳細なプライバシー情報を提供する。
- 予測や出力に関わるロジックを含め、AI ツール内で個人情報がどのように処理されるのか、また、AI の訓練やテスト、その他の開発のために個人情報をどのように使用するかを明確に知らせる。
- 例えば名前から性別や民族性を推測するなど、追加的な個人情報や特殊カテゴリーデータを作成する際には、その旨を明確に伝える。この処理に関する適切な合法的根拠と追加条件を特定する。
- 求職者から直接プライバシー情報を収集しない場合（例えば、求人ネットワーキングサイト、ソーシャル・メディア、その他の公開サイト、サードパーティーのデータベンダーなど）、その情報を入手してから 1 ヶ月以内にプライバシー情報を求職者に提供すること。妥当性確認が適用される場合は、そのアセスメントと正当性を十分詳細に文書化し、定期的に見直すこと。

採用担当者への勧告は以下の通りである：

- プライバシー情報をどのように求職者に提供するのか、また、どの当事者がその責任を負うのかを契約で明確に定める。
- 個人情報の取り扱い方法を受験者に知らせるため、詳細なプライバシー情報を提供すること。AI 提供者に指示する場合は、プライバシー情報が明確、正確、詳細であることを確認する。

□ 良い実務例：一部の AI 提供者は、受験者のスキルや行動を予測するためにゲームベースのアセスメントを行った。それらは加工業者であったが、ウェブサイトでいくつかのリソースを公開し、説明していた：

- アセスメントツールがどのように個人情報を処理したか。
- この情報を使って、どのように訓練し、ツールをテストしたのか。

リソースにはテキストとグラフィックの両方が含まれており、受験者にはアセスメントの招待状とともに、それらのリソースを案内していた。

ケーススタディ：組織 A は、面接の質問に対する候補者の書面回答を採点する AI ツールを AI 提供者として提供した。そのプライバシーポリシーには、処理に関する十分な詳細が含まれておらず、候補者を採用担当者のプライバシーポリシーに誘導していた。しかし、人材紹介会社のプライバシーポリシーは、候補者を組織 A のプライバシーポリシーに戻すよう指示していた。人材紹介会社との契約では、どちらが候補者に通知する責任があるのかが不明確であり、その結果、候補者はどちらの当事者からも十分な情報を得られなかった。組織 A は、中央 AI ツールの訓練とテストのために候補者の応募を匿名化し、バイアスを監視するために候補者の名前から人口統計学的特徴を推測する際の管理者であった。同社のプライバシーポリシーには、この処理に関する情報が非常に限られていた。したがって、彼らは候補者に通知せず、処理は事実上「不可視」であったため、英国の GDPR 第 5 条(1)(a)に違反する可能性が高い。

当団体は、管理者として個人情報を処理する前に、候補者に通知することを勧告した。また、求職者に全く通知しないことを避けるため、プライバシー情報を提供する責任が自社にあるのか、それとも人材紹介会社にあるのかを、契約書の雛形に明記することを勧めた。

採用担当者は、AI ツールを使用する前に、候補者に自分の情報がどのように処理されるかを通知する責任が誰にあるのかを確認し、それが行われていることを確認する必要もある。

ケーススタディ：組織 B は、候補者の大規模なデータベースを構築するために、一般の求人ネットワークサイトやデータベンダーから候補者のプロフィールを入手した。AI 検索ツールを使って、採用担当者の求人に関連するスキルや経験を持つ候補者を特定した。同社はウェブサイトでプライバシーポリシーを公開していた。しかし、英国 GDPR 第 14 条(5)(b)の「不釣り合いな努力」の適用除外に頼って、個人情報を処理・保存していることを積極的に知らせなかった。組織 B は各候補者の名前とメールアドレスを知っていたが、利用可能な選択肢を検討していなかった。そのため、プライバシー情報の AI 提供者が不釣り合いな労力を伴うことを正当化できなかった。

我々は、組織が積極的に 1 ヶ月以内に人々にプライバシー情報を提供すること、適用除外に頼る前に利用可能な選択肢をアセスメントすること、適用除外の決定を常に見直すことを勧告した。

採用担当者は、同様のサービスを利用する前に、潜在的な候補者が自分の情報がどのように処理されるかを知らされているかを確認すべきである。

詳細：

- 原則 (a)：合法性、公正性、透明性
- AI の透明性をどう確保するか？

- AI による決定を説明する
- プライバシー情報を提供するには、どのような方法があるか？
- 説明を受ける権利チェックリスト

AI におけるプライバシーのトレードオフ

AI ツールを開発または使用する際、考慮すべき価値や利益が異なる方向に引っ張られる可能性がある。我々は、組織が AI ツールを開発する際に、プライバシーと他の競合する価値や利益との間のトレードオフをどのように識別し、調整してきたかをレビューした。

AI 提供者は一貫して、プライバシーと他の競合する価値や利益との間の主要なトレードオフを以下のように特定している：

- 精度と説明のしやすさ - データポイントが増えれば出力の精度は向上するが、AI がどのように機能するかを人々に説明するのが難しくなることを含む。
- データの最小化対統計の正確性と妥当性 - より多くの個人データを収集・処理することで、アウトプットの正確性と妥当性を改善することができるが、必要以上の情報を収集することは、データの最小化の原則に準拠する可能性は低い。
- 透明性と理解しやすさ - プライバシー情報の中で AI を技術的に詳細に説明することは、透明性が高いように見えるかもしれないが、プライバシー情報が本当に理解しやすいかどうかに影響する。

考慮事項： 出力の精度は向上するが、透明性や説明性が低い複雑な機械学習モデルなど、利用可能な AI 手法の利点と限界をアセスメントする。

事例： AI ツールにおけるトレードオフの可能性は、通常、DPIA または AI 製品の仕様書に記録され、プロダクトマネージャーまたは法律顧問によって署名された。

しかし、いくつかの AI 提供者はトレードオフのアセスメントをどこにも記録しておらず、またトレードオフを検討したことを全く証明できない AI 提供者もあった。我々は、これらの AI 提供者に対し、AI ツールにおいてすべてのトレードオフを特定・評価し、DPIA などを選択したアプローチとその理由を文書化することを勧告した。

考慮事項： 設計上の考慮事項、決定事項、正当性を内部ウィキや技術文書に記録する。これらは、関連スタッフ、シニアリーダー、法律顧問がレビューし、ガイドとして使用することができる。

AI 提供者への勧告は以下の通りである：

- DPIA の一環として、個人情報のプライバシーとその他の競合する価値や利益との間の、AI ツールにおける潜在的・既存のトレードオフをすべて特定し、評価すること。それぞれのトレードオフについて、以下のことを行うこと：

- 利用可能なオプションを検討する；
 - 人々の権利と自由への影響をアセスメントする。
 - 選択したアプローチとその正当性を記録する。
- AI の設計と開発において、トレードオフを特定しアセスメントするプロセスを文書化する：
 - 人々のプライバシー権への影響をどのようにアセスメントするのか；
 - 誰に相談するか
 - トレードオフの決定を上級レベルで承認するのは誰なのか。
 - トレードオフ分析と決定を定期的に、特に AI や処理に変更を加える前に見直す。新しいトレードオフや新しい技術的アプローチを検討する。

採用担当者への勧告は以下の通りである：

- AI ツールにおいて、個人の情報プライバシーと他の競合する価値や利益との間のトレードオフの可能性および既存のトレードオフをすべて特定し、アセスメントすること。これは DPIA やプライバシーに対するより広範なアプローチの一環として行うこと。

□ **良い実務例**：ある AI 提供者は、採用担当者が候補者を次の選考段階に進める可能性を予測した。彼らは AI ツールを開発する際、精度は上がるが透明性や説明可能性が下がる複雑なモデルを使うなど、トレードオフをアセスメントしていた。彼らは、検討と決定を製品チケットに記録し、利害関係者がコメントを追加できるようにした。

ケーススタディ：組織 A は、候補者の大規模なデータベースから、採用担当者の求人に合致する候補者、または最も適した候補者を提案した。彼らは DPIA に主要な設計上の決定を記録していた。しかし、利用可能なアプローチのメリットとリスク、プライバシーと競合する利益のバランスをどのようにとったかは記録していなかった。また、場合によっては記録とは異なるアプローチを実際にとったこともあり、定期的な見直しや意思決定の更新も行っていなかった。

我々は、同組織に次のことを勧告した：

- 利用可能なアプローチと、その決断の理由を記録する；
- 新たなトレードオフや新たなアプローチを検討するため、定期的に更新・見直しを行う。
- このプロセスを開発ロードマップに記録することで、将来的に確実に実行できるようにする。

採用担当者は、DPIA の一環として、AI ツールのトレードオフも評価すべきである。

詳細：

- AI 関連のリスクをアセスメントする際、競合する利益をどのようにマネジメントすべきか？
- データの最小化と統計的正確さのバランスをどうとるべきか？
- AI におけるセキュリティとデータ最小化をどう評価すべきか？
- 公平性、バイアス、差別はどうか？

AI におけるヒューマンレビュー

我々は、英国 GDPR 第 5 条(1)(a)から(e)を遵守するために、AI のアウトプットまたは決定がどのように有意義にレビューされ、品質チェックされたかをレビューした。また、AI が法的またはそれに準ずる重大な影響を伴う自動化された決定を行ったかどうか、そしてこれが第 22 条に準拠しているかどうかも検証した。

ほとんどの AI 提供者は、AI アウトプットの人間によるレビューやサンプルなど、AI プロセスのある時点で人間の介入を入れている。

考慮事項： AI ツールの運用に密接に関与している認知行動や心理測定の専門家を参加させる。AI の出力を無作為にサンプリングし、公正、妥当性、正確性を確認する。

考慮事項： AI の出力について、ランダムレビューとリスクベースの人的レビューの両方を実施する：

- 不確かでありまいな入力；
- 予期せぬ、あるいは等級外の出力。
- ここで、パフォーマンス指標は潜在的なバイアスを浮き彫りにする。

事例： ヒューマン・レビューがプロセスの正式な段階である場合、レビューを行うスタッフは、何をチェックするか、どのように問題を特定し記録するか、どのような行動をとるかなどのレビュー方法について訓練を受けていた。

ヒューマン・レビューが公式化されていない場合、スタッフは一般的に訓練を受けておらず、一貫したレビューを徹底して行っていない。我々は、これらの AI 提供者に対し、レビューの一貫性を確保するために、人間によるレビューのプロセスを正式に文書化し、レビュー担当者に関連する訓練を提供することを勧告した。

この作業で検討された AI ツールは、人間の介入なしに自動化された採用決定を行うのではなく、人間の採用担当者の決定を支援することのみを目的として設計され、意図されていた。ほとんどの AI ツールは、指標となる成績や適合スコアを提供したり、人間の採用担当者が判断の際に考慮できる候補者の行動特性やスキルを示唆したりするだけであった。

考慮事項： AI の出力を使って自動的な採用決定を行わないようにする。人間の採用担当者が、AI が出力した指標グレードや適合スコアのみに基づいて候補者を進級させたり不合格にしたり

しないようにする。契約書、マーケティング資料、または採用担当者に提供する訓練やリソースに、使用目的を明確に記録する。

AI 提供者への勧告は以下の通りである：

- AI のアウトプットを確実に意味のある人間によるレビューや品質チェックにかけることで、アウトプットの正確性やバイアスの問題に早い段階で効果的に対処する。
- AI に意図せずエラーやバイアスを持ち込まないように、AI アルゴリズムの変更に関するサンプリングチェックを完全に行う。
- 完了したヒューマン・レビューや品質チェックの記録を残す。これには、実施した措置、行った変更、開発チームへのフィードバック、およびその理由や正当性を含む。
- どのような場合に人間がアルゴリズムを上書きできるのか、どのように管理者が人間のレビューをサンプリングしチェックするのかなど、AI の出力を人間がレビューするプロセスをポリシーに文書化する。

採用担当者への勧告は以下の通りである：

- AI ツールがこの目的のために設計されていない場合、採用担当マネジャーが AI のアウトプット（特に「適合性」や「適性スコア」）を使って自動的な採用決定を行わないようにする。
- AI ツールが自動判断を行う場合、候補者が自動判断に異議を唱えたり、異議を申し立てる簡単な方法を提供する。

□**良い実務例**：一部の AI 提供者は、採用担当者に候補者の志望理由書の各要素に対する目安の評点を与えていた。彼らは、評点が公正かつ正確であることを確認するため、評点の無作為サンプルと、AI が各要素をどのように採点し、重み付けしたかを検証した。また、採用担当者によって変更された評点を見直し、AI の採点における問題点や傾向を特定した。最後に、社内の利害関係者は、採用担当者が変更した成績の数およびその他の関連する成績指標を監視した。

ケーススタディ：組織 A は、候補者の大規模なデータベースを構築するために、一般の求人ネットワークサイトやデータベンダーから候補者のプロフィールを入手した。また、AI 検索ツールを使って、採用担当者の求人案件に関連するスキルや経験を持つ候補者を特定した。彼らは、AI 検索ツールの出力をレビューして、それが意図したとおりに機能しているかを確認することはしなかった。その代わりに、AI が提案した候補者がその求人に合わない場合は、採用担当者がフラグを立てるようにしていた。しかし、採用担当者にこのことを明確にしておらず、採用担当者がこのフィードバックを提供したり、エラーを指摘したりする仕組みを提供していなかった。

当組織は、AI のアウトプットに強固で有意義な人的レビューまたは品質チェックを導入し、早期に問題に対処できるようにすることを勧告した。また、採用担当者がエラーを報告し、レビューを受けるためのフィードバック・メカニズムを導入することも勧告した。採用担当者は、

AIがこの目的のために設計されていない場合、自動化された採用決定を行うためにAIツールを使用すべきではない。

詳細はこちら：

- [AIの意思決定における人間の監視の役割とは？](#)

DPIA とリスクマネジメント

AIツールは、ほとんどの場合、人々の権利と自由に高いリスクをもたらす可能性のある処理や革新的な技術を含むため、DPIAは法律で義務付けられている可能性が高い。我々は、組織がAIツールのDPIAを完了しているかどうかをチェックし、DPIAが有意義で詳細なものであることを確認するためにDPIAを見直した。また、英国GDPR第5条(2)、第24条～第25条、第35条～第36条を遵守するため、個人情報処理する前に、組織が個人を特定できる情報を特定し、そのリスクを軽減していることも確認した。

大半のAI提供者は、AIツールを個人情報処理に使用する前にDPIAを完了していた。しかし、一部のAI提供者は、DPIAを逆及的に、あるいは監査の直前に完了していた。DPIAのなかには日付が記載されていないものもあり、いつ完了したのか、あるいはいつ見直しが必要なのかは不明であった。

我々がレビューしたDPIAには通常、少なくとも以下の内容が含まれていた：

- 処理の目的と範囲の概要；
- 収集される個人情報の分野。
- 実施されているセーフガードの概要。

しかし多くの場合、DPIAは十分に詳細なものではなく、以下のような重要な要素が含まれていないことが多かった：

- AIシステムを通過するデータの流の詳細なマップである；
- データ保護の原則を満たす方法を検討する；
- 処理の必要性と比例性について意味のあるアセスメントを行うこと。
- 同じ結果を得るために、より少ない個人情報を使用する代替アプローチを検討する。

事例：いくつかのDPIAでは、人々に対する主なリスクや潜在的な影響のアセスメントが含まれ、これらのリスクを許容可能なレベルまで低減するための対策が提案されている。

新たなリスクやリスクの変更がどのように把握されたのか、あるいは、処理開始前に低減策が完全に実施され、有効であることを誰がチェックしたのか、不明確なことが多かった。我々は、DPIAとリスク軽減策を定期的にレビューし、コントロールが効果的に機能していることをチェックすることを勧告した。

考慮事項：組織にとってのリスクではなく、情報を処理することによる人々の権利と自由に対するリスクをアセスメントする。各リスクを軽減するための手段を特定し、実施する。

DPIA で一貫してアセスメントされてきた人に対する主なリスクは以下の通りである：

- AI ツールや処理操作に潜在的な異常が発生し、不正確な処理や出力が行われる可能性がある；
- AI ツールや訓練データに潜在的なバイアスがあり、その結果、処理や出力にバイアスが生じる；
- 不適切なスタッフやサードパーティが個人情報や AI のソースコードにアクセスすること；
- 個人データ漏えい、サイバー攻撃、または AI システムへのその他の干渉。
- 書面またはビデオによる回答において、収集の合法的な根拠と目的なしに、不必要な個人情報を誤って収集すること。

事例：ほとんどの AI 提供者は、社内の関係者が DPIA に関与していることを示唆していた。しかし、社内の専門家から受けたフィードバック、それをどのように検討したか、その結果何を変更したかについて明確に記録しているところはほとんどなかった。意図された処理について、特に個人情報の利用が合理的に期待され、透明性のあるものであるかどうかを調べるために、より広範な人々の意見を求めた AI 提供者はほとんどなかった。

AI 提供者は、社内外の関係者と有意義な協議を行い、その結果やフィードバックを検討し、協議後の変更を明確に記録することを勧告した。

考慮事項：プライバシー・コンプライアンス・ツールを使用して DPIA を完成させ、利害関係者のコメントを記録し、変更を追跡し、自動的にレビューを促す。

考慮事項：関連する方針、製品開発ロードマップ、プロジェクト・フローチャートに、DPIA のプロセスと DPIA を行う必要がある時期を文書化する。

DPIA には通常、社内のプライバシー・リーダーやデータ保護オフィサーを務めるスタッフからの助言が少なくとも含まれていたが、多くの場合、上級管理職による正式な承認は得ていなかった。

AI の AI 提供者は AI ツールの稼働後、ほとんどの DPIA を定期的に見直したり更新したりしていなかったり、いつ見直しが行われたか、何が変更されたかを明確に記録していなかった。その結果、以下のような問題があった：

- 識別されたリスクは変化していた；
- 軽減策をチェックし、それがまだ有効であるかどうかを確認した。
- アセスメントも軽減もまったくしていなかったプライバシーリスクが新たに発生したのだ。

考慮事項： AI または提案された処理に関する関連技術情報、または管理の証拠を AI 提供者に提供することにより、採用担当者が DPIA を完了できるよう支援する。手数料を請求することは、採用担当者の意欲を削いだり、リスクをしっかりとアセスメントすることを妨げたりする可能性があるため、行わないこと。

考慮事項： 新人採用担当者に訓練を提供し、AI ツールと出力の解釈方法を実演し、あるいはウェブサイトで参考ガイドやリソースを透明性をもって公開する。これにより、採用担当者が意図した方法で AI ツールを使用し、潜在的なプライバシーリスクを理解することをサポートする。

AI 提供者への勧告は以下の通りである：

- 人々の権利と自由に高いリスクをもたらす可能性のある情報処理を開始する前に、開発の初期段階から DPIA を完了させ、情報処理を行う前に DPIA を完了させる。
- プロセッサとして行動する場合であっても、AI またはその他の革新的な技術を使用する処理活動案については、DPIA の完了を検討すること。
- DPIA は、以下を含む包括的かつ詳細なものでなければならない：
 - 処理の範囲と目的
 - 各当事者間の関係とデータの流れを明確に説明すること；
 - どのように処理が英国 GDPR の原則に準拠するのか。
 - 代替アプローチの検討
- 低減後もなお、英国の人々の権利と自由に対するリスクが高い DPIA について、ICO の我々に相談する。
- DPIA を確実にレビューし、適切なシニアマネジャーが正式に承認すること（プライバシー・データ保護担当者など）。
- DPIA とリスク低減策を定期的に見直し、統制が効果的に機能していることを確認する。システム変更や情報処理の変更があった場合は、より頻繁にレビューを実施する。

採用担当者への勧告は以下の通りである：

- AI 採用ツールやその他の革新的技術の調達など、人々の権利と自由に高いリスクをもたらす可能性のある処理を開始する前に、DPIA を完了させること。
- DPIA は、以下を含む包括的かつ詳細なものでなければならない：
 - 処理の範囲と目的
 - 各当事者間の関係とデータの流れを明確に説明すること；
 - どのように処理が英国 GDPR の原則に準拠するか。
 - 代替アプローチの検討

- DPIA で人々の権利と自由に対するリスクを明確にアセスメントし、各リスクを軽減するための対策を特定し、実施する。
- 上記の勧告に従った明確な DPIA プロセスに従うこと。

ケーススタディ：組織 A は、受験者のスキルと行動を予測するためにゲームベースのアセスメントを AI 提供者として提供していた。彼らは AI ツールの各コンポーネントについて DPIA を完了していた。しかし、その内容は以下のような非常に軽いものであった：

- 彼らは、自分たちがコントローラーなのかプロセッサなのかを明確にしなかった；
- また、情報を保護するための技術的または組織的な措置についても説明しなかった；
- 他にもいくつかの異常や誤りがあった；
- いくつかの質問が「該当なし」とされたり、未完のまま残されたりした；
- 社内の利害関係者からのインプットはなかったが、社外の DPO からのハイレベルなアドバイスを含まれていた；
- リスクは人ではなく組織に関連するものであり、関連するスタッフは、実施すべき低減策を十分に認識していなかった。
- その間に AI ツールに何度か大きな変更があったにもかかわらず、彼らは 2019 年以降、AI ツールの見直しを行っていなかった。

DPIA が包括的で詳細なものであること、利害関係者との協議を含むものであること、人へのリスクについて定期的に厳密なレビューを行うことを勧告した。また、低減策を関連スタッフにコミュニケーションし、定期的にチェックすることを勧告した。

採用担当者はまた、詳細な DPIA を実施し、人に対するリスクを特定し、その低減策が実施され有効であることを定期的にチェックすべきである。

詳細：

- [データ保護影響アセスメント\(DPIA\)](#)
- [いつ DPIA を行う必要があるのか？](#)
- [DPIA はどのように行うのか？](#)
- [AI の DPIA を実施する際、何を考慮する必要があるのか？](#)

情報セキュリティと完全性

AI システムは、他の複数のソフトウェアコンポーネントやサードパーティーのシステムと統合される可能性が高く、より複雑なデータの流れを伴う。我々は、情報セキュリティ、完全性、アクセスリスクがどの程度効果的に管理されているか、また、英国 GDPR 第 5 条(1)(f)および第 32 条から第 34 条を遵守するために、AI ツールおよびその中の個人情報を保護するための適切な措置が講じられているかどうかをアセスメントした。

AI 提供者は通常、サードパーティーのインフラ上で AI ツールをホスティングしており、多くの場合、可用性リスクを最小限に抑えるため、固定容量のない「弾力的な」クラウドサーバーを使用していた。多くの AI 提供者は、特定の国や州のサーバーを採用担当者に提供することができた。これにより、データの収集から転送中までのデータ主権が維持された。

AI 提供者はインフラを監視するために、以下のような自動監視システムを導入していた：

- 脆弱性をスキャンする；
- リアルタイムのセキュリティ脅威を検知・分析する；
- 脅威の潜在的な影響を自動的に制限するために、限定的な是正措置をとる。
- 脅威に関するアラートを関連スタッフおよびシニアリーダーに報告する。

考慮事項：複数の監視・識別システムを「階層的」に運用し、システムが期待通りに機能していることを保証する。これにより、少なくとも 1 つのシステムが脅威を識別する可能性も高まる。

考慮事項：「バグバウンティ」を実施し、バグや脆弱性の可能性の報告を奨励することで、悪用される前に解決できるようにする。

AI 提供者は、AI ツールと個人情報を保護するために、さまざまな技術的管理を実施していた。ほとんどの場合、社内の情報セキュリティ・ポリシーやシステム運用ドキュメントに、これらを明確に文書化していた：

- 収集時、輸送時、保管時に、最低 AES256 ビットの対称型標準または同等の非対称型標準に情報を暗号化する；
- ネットワークに接続されているすべてのワークステーションとデバイスに、マルウェア、アンチウイルス保護、および組織で設定されたセキュリティソフトウェアをインストールする；
- ネットワーク・アクセス制限、ファイアウォール、侵入検知アラート、自動化されたリアルタイムのトラフィック監視とフィルタリング；
- 外部向け資産や重要または緊急のパッチを優先的に適用する、堅牢なパッチ適用プロセス；
- 製品開発と AI コード変更のテストに「サンドボックス」または別のテスト環境を使用することで、安全な開発を実践する；
- AI コード変更の独立した行ごとのレビューと、コード変更を展開する前の強固な承認プロセス；
- 情報資産のロギングやタグ付け、資産の安全な廃棄；
- 事業継続計画とフォールバック・プロセス
- 自動化されたフルバックアップと部分バックアップ、リストアプロセス。

考慮事項：脆弱性テストや侵入テストを含む、情報セキュリティマネジメントシステムの外部アセスメントを毎年実施する。また、AI 提供者を定期的に交代させ、調査結果が独立した公平なものとなるようにすることも検討する。

ほとんどの AI 提供者は、データ漏洩やニアミスをどのように調査、管理、報告するかを定めたデータ漏洩ポリシーや対応計画を持っていた。

考慮事項：個人データ漏えいプロセスを詳細に文書化する：

- 主要スタッフの責任
- 関連する違反を 72 時間以内に ICO に報告するという法定義務がある；
- 影響を受ける人々への通知プロセス
- コントローラまたはプロセッサとしてプロセスを区別する。

AI 提供者は通常、役割マップに基づいて、入社者、転職者、離職者にアクセス権限を割り当てている。これは、特定の職務に必要なシステムや個人情報への最低限のアクセス権を定めたものである。AI ツールやその中の個人情報へのアクセス許可は、通常、少数のシニア・リーダーのみに制限され、時間制限付きの接続制限などの追加管理の対象となっていた。

事例：いくつかのケースでは、AI 提供者が社内で役割を移動するスタッフのアクセス権の変更をどのように扱っているのか、また役割マップや既存のアクセス権をどのように定期的に見直しているのかが不明確であった。他のケースでは、アクセス、読み取り、編集、削除を含むユーザーの活動を自動的に記録していた。しかし、不適切なアクセスが発見されないように、ログを有意義に見直したり、自動監視の対象にしたりはしていなかった。

我々は、アクセスが適時に付与または変更され、アクセス管理プロセスが正式化されることを勧告した。また、不適切なアクセスの事例や傾向を特定するために、アクセス活動のログを定期的に見直すことを勧告した。

考慮事項：AI コードや個人情報へのアクセス権限など、AI システムに割り当てられたすべてのアクセス権限を定期的に見直す。

AI 提供者への勧告は以下の通りである：

- 技術的および組織的な管理を、どのように監視するかを含め、方針および契約に記録し、情報が最新かつ正確であることを確認するために定期的に見直す。
- セキュリティリスクや脆弱性をアセスメントし、発見事項とリスク対応策をリスク登録簿に記録する。定期的にレビューし、低減策が完全に実施され、有効であることを確認する。
- 主要な意思決定プロセスとスタッフの情報セキュリティ責任を、関連ポリシーとスタッフガイダンスに明確に文書化する。セキュリティに責任を持つスタッフが十分な訓練を受けていることを確認する。

- 従業員の端末に同等の技術的セキュリティ管理を実施し、管理が完全に維持されていることを監視し、少なくとも会社の端末と同じレベルで個人情報を保護する。
- データ侵害管理プロセスの有効性を実際にテストする。例えば、定期的にウォークスルー演習、デスクトップシナリオ、または主要スタッフによるシミュレーションを実施する。

採用担当者への勧告は以下の通りである：

- 技術的および組織的な管理が実施され、個人情報が収集時、輸送時、および保管時に安全であることの証拠を得ることを含む、意味のあるデューデリジェンスを実施する。
- 契約ライフサイクルを通じて定期的なコンプライアンス・チェックを実施し、技術的・組織的な統制が維持され、有効であることを保証する。
- 必要な技術的・組織的管理を、以下のように契約書に明記する：
 - アクセス管理を行う；
 - 変更管理プロセス
 - データ漏洩やニアミスが発生した場合の各当事者の責任を明確にする。

□ **良い実務例**：ある AI 提供者は、サードパーティと契約し、AI ツールとシステム・インフラストラクチャのセキュリティ・アセスメントを毎年 20~25 回実施していた。これによって、セキュリティ対策が適切かつ効果的に維持され、継続的にセキュリティが改善された。

詳細：

- サイバーセキュリティを含むセキュリティ
- 情報セキュリティ・チェックリスト
- 英国の GDPR データ侵害報告と自己アセスメント
- 個人データ漏えい：ガイド

経営フレームワーク

AI システムは、プライバシーとデータ・保護に対する明確な説明責任を伴う、組み込まれた管理フレームワークの中で開発されることが不可欠である。我々の監査では、以下を検証した：

- 組織が管理者または処理者としての責任をどのように果たしたか；
- 英国の GDPR 第 6 条、第 7 条、第 9 条を遵守するために、適切な処理の合法的根拠と、関連する場合は追加条件をどのように特定したか；
- 英国の GDPR 第 12 条から第 22 条を遵守するため、個人の権利要求を処理するプロセス。
- 英国 GDPR 第 5 条(1)(a)を遵守するために、効果的な上級指導者の監督、適切かつ適切なスタッフ研修、強固なポリシーがあったかどうか。

大半の AI 提供者は、特に AI ツールの開発と提供において、組織全体のシニア・リーダーによるデータ・プライバシー遵守の監督をサポートする明確なプライバシー管理の枠組みを証明することができた。AI 提供者はデータ・プロテクション・オフィサーを任命するか、プライバシーを担当するシニア・マネジャーを指名し、コンプライアンスを定期的にチェックし、KPI やパフォーマンス指標を監視し、シニア・リーダーにリスクを報告していた。また、ほとんどの AI 提供者は、データ保護の責任をスタッフの契約書や職務記述書に正式に記載し、データ保護コンプライアンスに対する合意されたアプローチをポリシーに記録していた。

考慮事項： プライバシーの知識をチェックし、ポリシーに対する意識を測定し、ギャップや関連する訓練を特定するために、定期的にスタッフの調査やテストを行う。

考慮事項： 製品チーム向けの「プライバシー・バイ・デザイン」訓練や、AI 技術者向けの「AI フェアネス」訓練など、主要なプライバシー責任を持つスタッフ向けの追加必須訓練を提供する。スタッフが定期的に訓練を更新し、関連知識を身につけるようにする。

考慮事項： 定期的なプロセスレビュー、内部または外部のプライバシーコンプライアンスアセスメント、プライバシーリスクのレビューを実施する。これにより、AI の管理環境を改善し、AI がプライバシーポリシーを遵守することを保証する。

英国の GDPR では、管理者は主な意思決定者であり、処理の目的と手段について全体的なコントロールを行使する。処理者は、管理者に代わり、管理者の指示に基づいてのみ個人情報を処理する。英国の GDPR では、管理者と処理者にはそれぞれ異なる責任と義務がある。組織は同時に、一部の処理活動については管理者となり、他の処理活動については処理者となることができる。あるいは、同じ個人情報を異なる目的で処理する場合、管理者と処理者の両方になることができる。

AI 提供者は、自社の AI ツールで個人情報を処理する際、管理者であるか処理者であるかを検討していた。いくつかの AI 提供者は、管理者または処理者としての役割を正しく判断していた。しかし、他の AI 提供者は、自分たちの役割を正しく、あるいはまったく決定していないことを証明することができなかった。

事例： AI スクリーニングまたは選考ツールの AI 提供者は、単一の中央 AI ツールを開発するために個人情報を処理する場合は管理者であり、採用担当者の指示に基づいて AI ツールを通じて候補者情報を処理する場合は処理者であると判断した。一部の AI 提供者は、採用担当者ごとに別バージョンの AI ツールを作成し、そのツールを採用担当者の候補者の個人情報のみで使用していた。これは、採用担当者の指示に従って行動する処理業者であり、採用担当者が処理の目的と手段を管理できることを示すものであった。

他の AI 提供者は、単一の中央 AI ツールを開発した。彼らは、AI を開発する際に、個人情報が実際にどのように処理されるのか、なぜ処理されるのかを決定したため、管理者となった。将来の採用担当者は、AI ツールを調達する前に行われた処理の管理者にはなり得ない。

事例： AI ソーシングツールの AI 提供者は、一般的に以下のように判断している：

- 管理者が候補者プロフィールのデータベースを構築し、検索アルゴリズムを開発するために個人情報を処理する場合。
- 候補者情報を処理し、採用担当者の指示に基づいて関連する候補者を斡旋する際の処理者。

考慮事項： もしあなたがコントローラーなら、あなたはコントローラーだ：

- 個人情報の処理手段および処理目的を全体的に管理する。
- 個人情報を独自の目的のために再度処理すること。

考慮事項： あなたが加工業者であるのは、次のような場合に限られる：

- 採用担当者は、処理の手段と目的について意味のある管理を行うことができる。
- 個人情報を自己の目的のために再度処理しないこと。

管理者として行動する AI 提供者は、一般的に処理の合法的根拠として正当な利益に依存していた。しかし、自社の利益と個人の利益およびプライバシーの権利とのバランスをとるための正当な利益のアセスメントを必ずしも完了していなかった。また、個人情報を処理していることを必ずしも人々に知らせていなかった。

一般的に、ほとんどの AI 提供者は、自社の AI ツールで個人情報を処理する合法的根拠として同意に頼っていなかった。

AI ツールの潜在的なバイアスを測定・監視するなど) データ管理者として特別カテゴリーデータを処理する場合、AI 提供者は推論情報を必ずしも特別カテゴリーデータとして扱っていなかった。この場合、処理に追加の条件が必要となるため、追加の条件なしに処理していた。合法的な根拠なしに個人情報を処理したり、合法的な根拠と追加条件なしに特殊カテゴリーデータを処理したりすることは、英国の GDPR では合法的である可能性は低い。

事例： ソーシングツールや候補者データベースを持つ一部の AI 提供者は、ソーシャルメディアや就職情報サイトで人々が明らかに公表している情報から推測されるという追加条件で、特別カテゴリーデータを処理していた。AI 提供者は、この追加条件が実際にどのように適切であるかを明確に説明または実証できなかった。

我々は、これらの AI 提供者に対し、推論された特殊カテゴリーデータを処理するための合法的根拠と追加条件を再考し、情報を処理する前に人々に通知するよう勧告した。また、適切な合法的根拠と追加条件を特定できない場合は、処理を中止し、情報を永久に削除するよう勧告した。

考慮事項：自社の採用活動に AI ツールを使用する場合、貴社は管理者であり、英国の GDPR 要件を満たす責任がある。これには、合法的根拠を特定すること、および特殊カテゴリーデータを処理している場合は追加条件を特定することが含まれる。

考慮事項：アセスメント後に任意のアンケートを実施し、候補者から直接人口統計学的特徴を収集し、明確な同意に基づいて処理する場合は、法律を遵守するために、同意を与えるのと同じくらい簡単に同意を撤回できるようにする。

AI 提供者への勧告は以下の通りである：

- 個人情報を処理する特定の事例ごとに、管理者であるか処理者であるかを特定する。プライバシー情報、契約書、DPIA、その他の文書に記録する。
- 処理を開始する前に、管理者として個人情報を処理する各事例について、合法的根拠を特定する。また、特別なカテゴリーのデータを処理する場合には、追加の条件を特定する。プライバシー情報、契約書、DPIA、処理活動の記録（RoPA）に記録する。
- 適切な合法的根拠を特定できない場合は、個人情報を処理しないこと。適切な合法的根拠と追加条件の両方を特定できない場合は、特殊カテゴリーデータを処理しないこと。
- すべての処理活動を詳細に記録した、定期的なデータ・フロー・マッピングに基づく RoPA を作成する。これには、目的、合法的根拠、追加条件、情報の共有先を含める。
- データ保護と AI のプライバシーのプロセスをポリシーに詳細に記録し、スタッフが情報を見つけ、責任を理解できるようにする。
- 個人の権利要求に従うためのプロセスを文書化し、実施する。これには、AI ツール内で個々の権利をどのように扱うか、採用担当者やその他の関連するサードパーティにどのように要望を伝えるかを含める。

採用担当者への勧告は以下の通りである：

- AI 提供者が個人情報を処理する各事例について、管理者または処理者としての役割が正しく特定されていることを確認する。プライバシー情報、契約書、DPIA、その他の文書に明確かつ一貫性をもって記録する。
- 管理者として処理の手段と目的を完全に管理し、処理を貴社の要件に合わせて調整できることを確認する。そうでない場合、AI 提供者が管理者または共同管理者となる可能性がある。
- 処理を開始する前に、個人情報を処理する各事例について、適切な合法的根拠を特定する。また、特別なカテゴリーのデータを処理する場合には、追加の条件を特定する。プライバシー情報、契約書、DPIA、RoPA に明確に記録する。
- 適切な合法的根拠を特定できない場合は、個人情報を処理しないこと。適切な合法的根拠と追加条件の両方を特定できない場合は、特殊カテゴリーデータを処理しないこと。

- すべての処理活動を詳細に記録した、定期的なデータ・フロー・マッピングに基づく RoPA を作成する。これには、目的、合法的根拠、追加条件、誰と情報を共有するかを含める。
- 定期的な内部プライバシー・コンプライアンス・チェック、KPI またはコンプライアンス指標の証拠を要求することにより、AI 提供者がプライバシー義務を遵守していることの保証を求める。
- 個人の権利要求が AI ツール内でどのように扱われるか、また、要求を AI 提供者やその他の関連するサードパーティにどのように伝えるかを検討し、文書化する。

□ **良い実務例**：一部の AI 提供者は、選考ツールを通じて、候補者の応募書類の各要素について、採用担当者に指標となる評点を与えていた。彼らは当初、個人情報を使用せずに AI ツールを開発し、各採用担当者に独自の AI ツールを提供した。そして、各採用担当者の指示に従って、その候補者の個人情報のみを使用して AI ツールの訓練とテストを行った。このような方法をとることで、1 つの中央 AI ツールの訓練やテスト、あるいは自社が管理者となる可能性が高いさらなる製品の開発のために、全採用担当者の個人情報を処理することはなかった。

ケーススタディ：組織 A はまた、採用担当者に対して、候補者の志望理由書の各要素に対する評点の目安を提供していた。AI ツールを開発するために個人情報を処理する場合、A 社は管理者であり、正当な利益を合法的根拠として特定したが、正当な利益のアセスメントは完了していなかった。また、採用担当者の指示により AI ツールで候補者の個人情報を処理する場合は、処理者であった。組織 A は、自社の採用に AI ツールを使用する際、まず処理の合法的根拠として同意に依拠した。

しかし、候補者の同意がない場合は正当な利益に依存することに戻したが、これは英国の GDPR に準拠していない。特別カテゴリーデータを処理するための追加条件は特定されていなかった。

当組織は、各処理活動に対して適切な合法的根拠を特定し、特殊カテゴリーデータを処理するための追加条件を特定することを勧告した。同意に依存する場合は、同意の仕組みが英国 GDPR 第 7 条の要件に準拠していることを確認し、同意が自由に与えられない場合は代替の合法的根拠に切り替えないことを勧告した。また、適切な合法的根拠と追加条件を特定できない場合は、処理を中止し、情報を永久に削除するよう勧告した。

ケーススタディ：組織 B は、候補者の大規模なデータベースを構築するために、一般の求人ネットワークサイトやデータベンダーから候補者のプロフィールを入手した。AI 検索ツールを使って、採用担当者の求人案件に関連するスキルや経験を持つ候補者を特定した。同社は、クライアントと契約する前に個人情報を処理して候補者データベースを作成し、クライアントから独立して AI 検索ツールの訓練とテストを行った。彼らは処理者であるため、この処理の合法的根拠を特定していないと判断した。組織 B と採用担当者は、契約においてそれぞれ処理者と管理者としての役割に合意していた。しかし、実際には組織 B が処理の手段と目的を管理してい

たため、実際には管理者であり、処理が英国の GDPR に準拠していることを確認していなかった。

採用担当者は、自分たちが採用される前に行われた処理を管理することは不可能であるため、データベースを作成する際には、自分たちが管理者であることを検討することを勧めた。その結果、同組織は、合法的根拠の特定を含め、英国 GDPR のあらゆる側面へのコンプライアンスを評価することを勧告した。

採用担当者は、契約において管理者となることに同意する前に、実際に処理の手段と目的を完全に管理できることを確認すべきである。

詳細：

- [原則 \(a\) : 合法性、公正性、透明性](#)
- [コントローラーとプロセッサ](#)
- [合法的根拠に関するガイド](#)
- [カテゴリー別データ](#)
- [AI における合法性をどのように確保するのか？](#)
- [英国 GDPR 第 30 条では何を文書化する必要があるのか？](#)
- [説明責任の枠組み](#)
- [AI の説明責任とガバナンスにはどのような意味があるのか？](#)
- [AI システムにおいて個人の権利をどのように確保するのか？](#)

サードパーティとの関係

AI システムは複雑なデータサプライチェーンを含む可能性がある。我々は、英国の GDPR 第 5 条(1)(e)および(f)、ならびに第 24 条から第 29 条を遵守するために、明確なデータ保護責任を定めた契約書が存在し、すべての関係者がそれに従っていることを確認した。

AI 提供者は通常、採用担当者と契約またはデータ処理契約を結んでいた。AI 提供者がプロセッサである場合、採用担当者からの明示的な処理指示は契約書に含まれていたが、多くの場合、大雑把な表現で、従うべき原則のみを網羅していた。

事例：我々が目にしたいいくつかの契約書は、あまりにも大まかで、具体的な詳細が十分に含まれていなかった。例えば、以下のような十分な情報が含まれていなかった：

- [どのような個人情報をどのように処理するのか；](#)
- [各当事者の責任](#)
- [各当事者が実施する技術的・組織的措置、あるいは](#)
- [契約が終了した場合、AI モデルの情報をどのように扱うのだろうか。](#)

我々は、これらの AI 提供者に対し、上記の必要な詳細およびデータ保護条項をすべて含むように契約を改訂することを勧告した。

考慮事項：各当事者のデータ管理者およびデータ処理者の義務を明確に定め、提案する個人情報の処理について透明性をもって説明する契約において、平易な言語によるデータ保護条項を使用する。

契約は多くの場合、AI 提供者が作成したテンプレートに基づいており、採用担当者との顧客契約プロセスの一環として合意されていた。契約は通常、どちらかの当事者が積極的に解約するまで有効であった。多くの AI 提供者と採用担当者は、契約条件と明示的な処理指示が適切であり、目的に合っているかをチェックするために、契約の定期的な見直し（通常は年 1 回）を組み込んでいた。

考慮事項：採用担当者が契約条件や処理指示の追加、変更、削除を自社のニーズに合わせて行えるようにする。特に、採用担当者が同意するための標準的な契約書テンプレートを AI 提供者が提供する場合。採用担当者が処理の手段と目的を実質的に管理できない場合、または AI 提供者が実務上これを決定する場合、AI 提供者は処理者ではなく管理者となる。

事例：AI 提供者は、インフラやセキュリティ、カスタマーサポート・プラットフォーム、メッセージング・サービスなど、AI ツールのために独自のプロセッサと契約していた。AI 提供者は通常、少なくとも同等の防御を伴う契約書を交わしていた。しかし、契約に合意した後、追加のサブプロセッサを雇用する前に、採用担当者から書面による承認を得ていることを必ずしも示すことができなかった。

我々は、AI 提供者が追加のサブ・プロセッサを雇う前に、明確な書面による承認を得ること、そしてこのプロセスを契約に追加することを勧告した。

AI 提供者は通常、プロセッサと契約する前に、少なくとも何らかのデューデリジェンスを行っていた。AI 提供者は、技術的な対策が実施されていることを証明するために、継続的にコンプライアンスを証明する書類を受け取り続けていた。

考慮事項：採用担当者が確認できるように、デューデリジェンスや継続的なコンプライアンスに関する証拠をポータルやウェブサイトで積極的に公開する。

考慮事項：公的情報源（求人サイト、ソーシャルメディア、ネットワーキング・サイトなど）から個人情報を大量に取得する場合は、サードパーティやデータ・ベンダーとの契約に合意する。これらの契約には、処理の合法性と透明性、および収集した当初の目的との適合性を明確に定める。大規模なデータセットがデータ保護法を遵守していることを確認するために、デューデリジェンスや継続的なチェックを行うことを検討する。

AI 提供者への勧告は以下の通りである：

- 管理者または処理者としての各当事者の責任と、提案された処理の詳細について明確に規定した、期限付きの書面による契約またはデータ処理契約に合意する。
- 以下の明示的な処理指示を確実に行う：
 - 処理する特定の個人情報、
 - 処理方法とその理由、
 - アウトプットの内容、
 - 保存方法、
 - 保存期間、
 - 共有する相手、
 - 保護措置の内容。
- 採用担当者およびサブプロセッサーとの契約を定期的に見直し、正確かつ十分であり、目的に適合していることを確認する。
- サブプロセッサーが契約を遵守していることを確認する。日常的なコンプライアンスチェックを実施したり、契約条件や処理指示に従っていることの証拠を要求する。
- 契約書、顧客導入プロセス、プロジェクト管理プロセス、およびシステム調達方針において、データ処理契約またはデータ保護条項の要件を文書化する。

採用担当者への勧告は以下の通りである：

- 管理者または処理者としての各当事者の責任と、提案されている処理の詳細について明確に規定した、期限付きの書面による契約またはデータ処理契約を締結する。
- 以下の明示的な処理指示を確実に行う：
 - あなたが処理している特定の個人情報；
 - どのように、そしてなぜそれを処理するのか；
 - 出力はどうなるのだろう；
 - どのように保管するのか；
 - それをどのくらいの期間保持するのか；
 - 誰と共有するのか。
 - どのような保護措置が取られるのか。
- 管理者として、処理の手段および目的を完全に管理できるようにする。標準契約または明示的な処理指示を、貴社のニーズに合わせて有意義に変更できるようにする。
- AI 提供者との契約を定期的に見直し、契約が正確かつ十分で、目的に合っていることを確認する。
- AI 提供者が契約を遵守していることを確認する。これは、日常的なコンプライアンス・チェックを行うか、契約条件や処理指示に従っていることの証拠を要求することによって行う。

□ **良い実務例**：一部の AI 提供者は、面接の質問に対する候補者の書面回答を自動的に採点する AI ツールを使用していた。また、採用担当者がそれぞれのニーズに合わせてカスタマイズできる契約書のテンプレートを使用している。これには詳細なデータ保護条項と責任が含まれている。契約書の署名入りコピーを保管し、条件を迅速にチェックできるようにしている。

ケーススタディ：組織 A は、受験者のスキルと行動を予測するためにゲームベースのアセスメントを AI 提供者に依頼した。契約書の雛形はあったが、AI ツールと処理に関する非常に大まかな情報しか含まれておらず、従うべき明確な指示は含まれていなかった。また、契約書には、AI ツールや他の製品を開発するために受験者情報を再利用するなど、組織 A 独自の目的のための追加処理についても触れられていなかった。また、契約条件が適切であり、遵守されていることをチェックするために、契約を定期的に見直していなかった。

当組織は、契約に詳細な情報と具体的な処理指示を盛り込み、定期的に見直すことを勧告した。

採用担当者はまた、詳細かつ具体的な契約のみに合意し、AI 提供者が契約を遵守していることの保証を求めるべきである。

詳細：

- [AI におけるコントローラーとプロセッサの関係](#)
- [コントローラとプロセッサ間の契約と責任](#)
- [契約書には何を記載する必要があるのか？](#)
- [プロセッサにはどのような責任と義務があるのか？](#)