AMT/NEWSLETTER

IP & Technology

2026 年 5 月 29 日

ヨーロッパ・オセアニアの最新法制度動向（欧州・英国当局による X/Grok 関連リスクへの調査・執行動向、AI 技術の進歩と規制の進化（ディープフェイク、AI エージェント）及びオーストラリアを中心とする未成年者の SNS 利用規制の動き）

弁護士　中崎 尚

Contents

イーロン・マスク氏との対立を深める欧州各国は、同氏と関係の深い xAI 社の Grok に対して、強い姿勢を見せています。また、欧州では、ディープフェイクに対して厳しい規制が行われる一方で、AI 技術の進化に対応すべく、AI エージェントの規律の在り方の検討が進められています。同時に、延期の可能性があるものの、EU と EU 加盟国では、EU AI 法の全面施行に向けた準備が進められています。

オーストラリアでは世界に先駆けて未成年者の SNS 利用を禁止する制度が導入され、他法域での議論にも影響を与えています。

本ニュースレターは、「GLOBAL LAW UPDATE ヨーロッパ・オセアニアの最新法制度動向（AI・データ保護・プライバシー関連）」（2026 年 3 月 BUSINESS LAWYERS LIBRARY 掲載）（2026 年 3 月 4 日時点での情報に依拠）の内容をベースとしております。

1. 欧州・英国当局による X/Grok 関連リスクへの調査・執行動向

Q1. 欧州各国による、X/Grok 関連リスクへの調査・執行が進んでいますが、AI・データ保護分野ではどのような動きがありますか？

2026 年 1 月 26 日、欧州委員会はデジタルサービス法（以下「DSA」）に基づき、Grok 機能の導入等に伴うシステミック

リスクに関して X 社に対する新たな調査を開始すると同時に、2023 年 12 月に開始した同社のコンテンツ推薦・表示順位付けシステムに関する現行手続を延長することを発表しました。また、英国でも、英国データ保護機関（以下「ICO」）が、xAI 社の開発する AI システム「Grok」に対する調査を開始しました。

（1） 欧州委員会による調査の開始

欧州委員会は、X 社が DSA に基づく以下の義務を遵守しているかどうかについて調査していることを公表しました[1]。

- 以下のシステム上のリスクを注意深く評価し軽減できているか
  - 違法コンテンツの拡散
  - ジェンダーに基づく暴力に関連する悪影響
  - プラットフォーム上での Grok 機能の導入による身体的・精神的健康への深刻な悪影響
- Grok の機能が X（X 社の運営するソーシャルネットワーキングサービス）の全体的なリスクプロファイルに重大な影響を与える場合、導入前にリスク評価報告書を作成し委員会に提出できているか

また、欧州委員会は、別途、2023 年 12 月に開始していた手続を延長し、X 社がコンテンツ推薦・表示順位付けシステムに関連する全てのシステミックリスク（Grok ベースの同システムへの最近の移行の影響を含む）を適切に評価・軽減したかどうかを審査しています。

欧州委員会によれば、これらの不備は DSA 34 条（1）、34 条（2）、35 条（1）、及び 42 条（2）の違反に該当する可能性があります。欧州委員会は、X のサービスに実質的な改善が見られない場合、引き続き証拠収集を継続し、暫定措置を課す可能性があるとしています。

（2） 英国による調査の開始

2026 年 1 月 7 日、ICO は、Grok に関する声明を発表しました[2]。続けて同年 2 月 3 日、ICO は、X Internet Unlimited Company（以下「XIUC」）及び xAI 社に対し、Grok の AI（人工知能）システムに関連する個人データの処理、及び有害な性的画像・動画コンテンツを生成する可能性について、正式な調査を開始したと発表しました[3]。

ICO は、Grok が個人の同意を得ていない性的画像を生成するために使用されたとの報告を受け、英国のデータ保護法上の懸念があり、かつ公衆に重大な危害をもたらす潜在的なリスクが生じているとして、調査を開始しました。ICO が懸念しているのは、個人データが合法的、公正かつ透明性をもって処理されたかどうか、また個人データを用いた有害な改変画像の生成を防ぐための適切な安全対策が Grok の設計と展開（デプロイ）に組み込まれていたか否かという点です。ICO は、現時点では、調査に着手したのみであり、xAI 又は XIUC によるデータ保護法違反の十分な証拠があるか否かについて、一定の見解に達しているわけではないとしています。

2026 年 1 月 12 日、英国の科学・イノベーション・技術担当国務大臣は、X における Grok の最近の使用に関する懸念と政府の対応計画を概説する声明を下院に提出しました[4]。ポイントは 3 点あります。

① この声明で大臣は、同意なしにディープフェイクによる性的・裸体等の私的状態にあるように見える画像（以下「性

---

1 https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203（2026 年 5 月 26 日最終閲覧）

2 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/01/a-statement-in-response-to-grok-ai-on-x/（2026 年 5 月 26 日最終閲覧）

3 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/02/ico-announces-investigation-into-grok/（2026 年 5 月 26 日最終閲覧）

4 https://www.gov.uk/government/speeches/secretary-of-state-statement-to-the-house-of-commons-12-january-2026（2026 年 5 月 26 日最終閲覧）

的画像等」）を流出させたり、流出させるぞと脅迫したりする行為は、個人については刑事犯罪となり、プラットフォームについては Online Safety Act 上、当該違法コンテンツに関するリスク評価、予防、削除等の義務・執行対象となると強調しています。さらに、2025 年に成立した Data (Use and Access) Act 2025 第 138 条による Sexual Offences Act 2003 の改正（66E～66H の追加）により、同意（又は同意があると合理的に信じるだけの事情）がないまま、「purported intimate image of adult（成人が性的・裸体等の私的状態にあるように見える非真正画像）」を作成すること又は作成を依頼することが犯罪化されたことも記載されています。

② また、この声明で大臣は、英国の通信・放送・オンラインサービスを所管する規制機関（Office of Communications、以下「Ofcom」）が X に対する正式な調査を開始し、Online Safety Act の遵守状況を評価していることが確認されています。なお、公表時点で、Ofcom は、現時点で xAI を調査していない、スタンドアロンの Grok サービスによる違法画像の作成自体については Online Safety Act の構造上この件では調査できない、としている点は注意が必要です。

③ さらに、この声明で大臣は、2026 年 1 月 12 日の声明時点で議会審議中であった Crime and Policing Bill。なお Crime and Policing Bill（犯罪対策・警察法案）を通じ、ヌード化（ヌード画像への改変）アプリの提供を犯罪として取り扱う強い意向を明らかにしました。実際に、同法案は 2026 年 4 月 29 日に Royal Assent を受け、Crime and Policing Act 2026 として法制化されました[5]。これにより、同意のない性的画像を作成するツールの提供が禁止されることになります。加えて、同声明で、大臣は、テクノロジー企業に対し、オンライン上の女性と少女の安全向上に関する Ofcom の指針で推奨されている措置を実施することを求めています。

2. ディープフェイクに対する規制動向

Q2. 欧州各国のディープフェイクに対する規制動向を教えてください。

ディープフェイク規制の充実化に向けて、EU 加盟国で活発な動きが見られます。ポーランドのデータ保護当局（UODO）は、国内法改正の必要性を訴え、イタリアのデータ保護当局（Garante）は、AI コンテンツ生成サービスの提供者に対し、ディープフェイク対策の実施を求めています。またアイスランドとフランスのデータ保護当局は、ディープフェイク対策のガイドラインを公表しました。

（1） ポーランド

2026 年 1 月 27 日、ポーランドのデータ保護当局（以下「UODO」）の長官は、欧州司法裁判所（CJEU）の 2025 年 12 月 2 日判決 Russmedia Digital and Inform Media Press（C-492/23）（以下「Russmedia 判決」）[6] を踏まえ、ディープフェイク対策のためにポーランド国内法の改正が必要であるとの見解を示しました[7]。Russmedia 判決は、ルーマニアのオンライン広告サイトに、本人の同意なく女性の写真と電話番号を用い、その女性が性的サービスを提供しているかのような虚偽広告が掲載された事案に関するものです。CJEU は、広告がユーザーによって投稿されたものであっても、オンライン・マーケットプレイス運営者が当該広告に含まれる個人データの公開・配信の方法に影響を及ぼし、自らの商業的・広告的目的のためにも処理している場合には、GDPR 上の管理者となり得ると判断しました。

---

5 https://bills.parliament.uk/bills/3938（2026 年 5 月 26 日最終閲覧）

6 https://curia.europa.eu/site/upload/docs/application/pdf/2026-01/monthly_case-law_digest_en-_december_2025.pdf（2026 年 5 月 26 日最終閲覧）

7 https://uodo.gov.pl/pl/138/4055（2026 年 5 月 26 日最終閲覧）

同判決は、特にセンシティブデータを含む広告について、プラットフォーム運営者が掲載前に当該広告を識別し、広告投稿者がデータ主体本人であるかを確認する必要があるとしました。投稿者が本人でない場合には、本人の明示的同意または GDPR 上の他の例外が示されない限り、運営者は当該広告の掲載を拒否しなければならないとされています。また、運営者には、掲載されたセンシティブデータを含む広告が他のウェブサイトに不法にコピー・再公開されることを防ぐため、適切な技術的・組織的安全管理措置を講じる義務もあるとされました。さらに、運営者は電子商取引指令上のホスティング等の仲介者責任免除を根拠として、GDPR 上の管理者義務を免れることはできないと判断されています。

UODO は、この判決が、オンライン広告サイトにとどまらず、SNS を含むオンラインサービスの責任評価にも重要な意味を持つと位置付けています。UODO によれば、こうしたサービスは、個人データを保存・公開するだけでなく、投稿・拡散のための技術的手段を提供しており、その意味で単なるホスティング提供者にとどまらない側面があります。UODO は、この解釈が、特に未成年者の画像、AI によって生成された偽写真・偽録音、著名人の肖像を用いた偽広告など、ディープフェイク被害に対するより強い保護の必要性を示すものだとしています。

UODO は、ポーランドの著作権法、民法、刑法および GDPR が、肖像、声、人格権、個人データ等について一定の保護を与えることを認めつつも、現行のポーランド法は、ディープフェイクのような現代的技術の特性と複雑性に直接対応していないと指摘しています。また、EU AI 法やデジタルサービス法（DSA）もディープフェイク問題に触れているものの、違法なディープフェイク素材の削除等を含む包括的な保護制度としては不十分であり、国内法による補完が必要であるとしています。

さらに UODO は、2025 年 9 月にポーランドのデジタル化担当大臣に対し、ディープフェイクの悪影響から実効的に保護するための法的措置の検討を求めたこと、同年 12 月の回答では電子サービス提供法の改正により違法オンラインコンテンツへのアクセス遮断命令等が予定されていることを紹介しています。しかし UODO は、この改正案はディープフェイク対策に特化して設計されたものではなく、プライバシーおよびその他の基本権を実効的に保護するには不十分であると評価しています。

最後に UODO は、AI を使用して作成された児童搾取素材やグルーミング事例が急増していることを挙げ、有害な AI 生成コンテンツから未成年者を保護することを最優先すべきだと結論付けています。

（2）イタリア

2026 年 1 月 8 日、イタリアのデータ保護当局（Garante）は、2025 年 12 月 18 日付 2025 年 12 月 18 日付 Garante 決定（Provvedimento n. 789 / Delibera）（以下「789 号決定」）[8]を発令したことを公表しました。この規定には、AI（人工知能）サービスの利用者に対するディープフェイクに関する警告が含まれています。

789 号決定は、デジタルマルチメディアコンテンツを生成する AI サービスが個人データ（特に音声や画像）を処理すること、また当該データがサービス利用者以外の第三者に帰属する可能性があり、当該第三者が自身の個人データ処理を認識していない場合があることを強調しています。さらに、AI ツールを用いて処理されたデータが、詐欺、名誉毀損、なりすましを目的とした欺瞞的な使用など、違法な目的で利用される可能性により、当該処理に伴う高いリスクがさらに増幅されることを指摘します。

また、同決定は、データ管理者又は処理者として、第三者の実在の声や画像を素材として AI によるコンテンツ生成サービスを利用する全ての自然人又は法人に対し、適法な根拠なく、かつデータ主体に正確かつ透明性のある情報を事前に提供せずに実施される個人データの処理は、EU の一般データ保護規則（GDPR）5 条（1）（a）、6 条、及び 9 条に違反する可能性が高いと警告しています。

このようなサービス利用者に対する警告に加えて、第三者の音声や画像を利用したコンテンツ生成 AI サービスの利用者及び提供者に対し、利用者がデータ保護義務を履行できるよう、アプリケーション・サービス・製品の開発、設計、選定、提供の各段階において、配慮を求めています。

[8] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10207132（2026 年 5 月 26 日最終閲覧）

（3）フランス

2026 年 2 月 3 日、フランスのデータ保護機関（CNIL）は、AI（人工知能）技術により生成又は加工された音声・画像・動画、いわゆるディープフェイク又は「hypertrucage」について、リスク、違法コンテンツへの対応方法、個人データ保護上の救済手段を説明する記事を公表しました[9]。CNIL は、ディープフェイクを、AI 技術により作成又は改変された音声・写真・動画であり、声、顔、動きの模倣や、完全又は部分的に架空の画像・動画の作成を可能にするものと説明しています。

CNIL は、AI 生成又は加工された音声・画像・動画を含むディープフェイクが、プライバシー侵害、本人の評判の毀損、なりすまし、セクストーション、サイバーハラスメント、詐欺、偽情報・世論操作、ヘイトコンテンツや児童ポルノ的コンテンツの生成といった深刻な被害をもたらし得ると説明しました。CNIL はまた、本人の同意なく人物の画像を加工する行為、ハラスメント、詐欺、AI ツールで作成された児童ポルノ的コンテンツの作成・流通等が、フランス法上、罰金又は複数年の拘禁刑の対象となり得ることを示しています。

生成 AI 一般について、CNIL は別途、生成 AI システムが画像・文章・コード等の生成、既存コンテンツの再処理、データ分析に利用される一方、もっともらしいが不正確な出力、過度な信頼による誤った判断、ブラックボックス性、バイアス、ディープフェイクを通じた偽情報などの濫用リスクを伴うと説明しています[10]。この点は、2 月 3 日のディープフェイク記事に加え、CNIL の生成 AI に関する FAQ を補足根拠として位置づけることができます。

さらに CNIL は、特定可能な個人の顔、声、氏名などの個人データが本人の同意なく使用された場合、CNIL に苦情を申し立てることができると説明しています。ただし、CNIL への苦情申立ては、警察又は憲兵隊への刑事告訴に代わるものではなく、CNIL は被害者のために損害賠償を取得したり、犯罪・軽罪の加害者に刑事制裁を科したりする機関ではないとも明記しています。

企業に関しては、CNIL の 2 月 3 日の記事が個人向けの注意喚起を中心としている点に留意が必要です。一方で、CNIL の生成 AI FAQ は、企業その他の組織が生成 AI システムを導入する場合、事前のリスク分析、明確なガバナンス戦略、GDPR 適合性の確認、提供者との役割分担や契約関係、域外移転の管理、入力データ及び利用データの安全確保を検討すべきであるとしています。また、内部ポリシー又はチャーターにより許可される利用と禁止される利用を明確化し、機密情報又は個人データの入力制限、利用者教育、定期的な管理を行うことが推奨されています。

さらに、ディープフェイクや AI 生成コンテンツの透明性については、EU の AI Act に基づく規律も関連します。欧州委員会は、AI Act 第 50 条が生成 AI・対話型 AI・ディープフェイクを含む一定の AI システムの提供者及び導入者に透明性義務を課すものであり、欺罔、なりすまし、誤情報のリスクを低減し、利用者が AI とやり取りしていること又は AI 生成コンテンツに接していることを理解して、情報に基づく判断を行えるようにすることを目的としていると説明しています[11]。具体的には、AI 生成又は加工コンテンツの機械可読なマーキング、関連する検出メカニズム、ディープフェイク又は公共の利益に関する AI 生成・加工テキストについて AI 由来であることを知らせる義務が問題となります。

3. AI エージェントの規制

Q3. 欧州での AI エージェント・エージェンティック AI の規制動向を教えてください。

---

9 https://www.cnil.fr/fr/hypertrucage-deepfake（2026 年 5 月 26 日最終閲覧）

10 https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-lutilisation-dun-systeme-dia-generative（2026 年 5 月 26 日最終閲覧）

11 https://digital-strategy.ec.europa.eu/en/faqs/guidelines-and-code-practice-transparent-ai-systems（2026 年 5 月 26 日最終閲覧）

（1） 英国

2026 年 1 月 8 日、英国の ICO は、エージェンティック AI に関する報告書「ICO tech futures: Agentic AI」を発表しました[12]。この報告書で ICO は、エージェンティック AI に関する ICO の現時点での理解、潜在的な利用・技術発展、組織が導入を検討する際に考慮すべきデータ保護上の影響、リスク及び機会を明らかにしています。ただし、ICO は同報告書を正式なガイダンスまたは規制上の期待事項ではないと位置付けています。

ICO は、エージェンティック AI について、同日ニュースリリースで、エージェンティック AI を「より多くの活動を自動化し、意思決定を行い、環境と相互作用し、リアルタイムで問題を解決し、ある種の推論や計画を模倣する AI」と定義した上で、エージェンティック AI は、新たな技術的能力を提供する一方で、まだ開発の初期段階にあり、多くのユースケースが実証されていないか開発中であると指摘しています。特に、エージェンティック AI のデータ保護リスクとして報告書は以下のリスクを指摘しています。

- AI のサプライチェーンにおける管理者（コントローラー）と処理者（プロセッサー）の責任範囲の確定に関する問題
- 複雑化するタスクの急速な自動化による自動意思決定量の増加
- 処理目的が広範に設定されているために、無制限のタスクや汎用型エージェントが許容されてしまうこと
- 指示や目的達成に必要な範囲を超えて個人情報が処理されるおそれ
- 特別カテゴリーのデータ（センシティブデータ等）の意図しない使用や推論の可能性
- 透明性や情報権利行使の容易さに影響する複雑性の増大
- エージェンティック AI の性質に起因する新たなサイバーセキュリティ上の脅威
- パーソナルアシスタントエージェントの利用を促進する個人情報の集中化

（2） フィンランド

2026 年 1 月 28 日、フィンランド交通通信庁（Traficom）は国家緊急供給庁（Huoltovarmuuskeskus）とともに、AI エージェントのサイバーセキュリティに関するガイダンス「Tekoälyagenttien kyberturvallisuus」を公表しました。同ガイダンスは、組織が AI エージェントを安全に設計、調達、テスト、運用する際のサイバーセキュリティ上の考慮事項を整理しています[13]。

同ガイダンスは、OWASP Top 10 for Agentic Applications（2026）及び LLM Top 10（2025）をフレームワークとして参照し、セキュリティ・バイ・デザインの実務を、リスク評価、脅威モデリング、データガバナンス、プロンプト・ツールの強化、継続的テスト/監視の観点から、EU AI 法上の要求事項との関係も踏まえて説明しています。

4. ヨーロッパの AI 規制の動向

Q4. ヨーロッパの直近の AI 規制動向を教えてください。

（1） AI 分野のデジタルオムニバス提案のその後

2026 年 1 月 20 日、欧州データ保護会議（European Data Protection Board。以下「EDPB」）及び欧州データ保護監督官（European Data Protection Supervisor。以下「EDPS」）は、欧州委員会が 2025 年 11 月 19 日に公表した AI 分野のデジタ

12 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/01/ai-ll-get-that/（2026 年 5 月 26 日最終閲覧）

13 https://www.traficom.fi/fi/ajankohtaista/tekoalyagentit-muuttavat-kyberuhkia（2026 年 5 月 26 日最終閲覧）

ルオムニバス提案（Digital Omnibus on AI）[14]について、EDPB-EDPS 共同意見書 1/2026 を採択しました[15]。同意見書は、EDPB により 2026 年 1 月 21 日付で公表されています。

同提案は、EU AI 法の実施を簡素化するため、AI リテラシー義務、バイアス検出・修正のための特別カテゴリーの個人データ処理、高リスク AI システムに関する一部義務の適用時期等について改正を行うものです。

その後、理事会は 2026 年 5 月 7 日、理事会議長国と欧州議会の交渉担当者が暫定合意に達したことを公表しました[16]。なお、5 月 13 日付理事会文書 9247/26 によれば、当該暫定合意は 2026 年 5 月 6 日に交渉当事者間で成立し、同月 13 日に COREPER により確認されたものです[17]。正式採択には、欧州議会及び理事会による承認が必要ですが、本ニュースレターでは速報として重要なポイントをご紹介します。

i. バイアスの検出・修正のための、特別カテゴリーの個人データの処理

欧州委員会の当初提案は、EU AI 法 10 条 5 項を新たな 4a 条に置き換え、バイアスの検出・修正のために必要な場合には、一定の保護措置を条件として、特別カテゴリーの個人データの処理をより広く認める内容でした。これに対し、EDPB 及び EDPS は、2026 年 1 月の共同意見書において、このような処理は例外的なものにとどめられるべきであり、厳格な必要性、代替手段の不存在、適切な技術的・組織的保護措置、データ保護法上の監督権限との整合性が確保される必要があると指摘しました[18]。

5 月の暫定合意では、この点について「厳格に必要な場合」という基準が明記されています。高リスク AI システムの提供者については、AI 法 10 条 2 項(f)及び(g)に基づく健康・安全に影響を及ぼす可能性がある、基本権に悪影響を及ぼす、又は EU 法で禁止される差別につながる可能性があるバイアス検出・修正のために厳格に必要な範囲で、また、その他の AI システム及びモデルの提供者・導入者並びに高リスク AI システムの導入者については、健康・安全、基本権又は差別禁止に重大な影響を及ぼし得るバイアスの検出・修正のために厳格に必要な範囲で、特別カテゴリーの個人データの処理を例外的に認める構成とされています。また、少なくとも上記の拡張対象となる提供者・導入者について、当該規定自体がバイアス検出・修正を実施する新たな義務を創設するものではないことも明記されています[19]。

また、暫定合意では、合成データ又は匿名化データ等では目的を達成できないこと、再利用を制限する技術的制約を設けること、最先端のセキュリティ及びプライバシー保護措置を講じること、アクセス管理及び守秘義務を確保すること、第三者への移転・アクセスを禁止すること、バイアス修正後又は保存期間満了後にデータを削除すること、厳格な必要性及び代替手段がない理由を記録すること等が保護措置として掲げられています[20]。

---

14 https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal（2026 年 5 月 26 日最終閲覧）

15 https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf（2026 年 5 月 26 日最終閲覧）

16 https://www.consilium.europa.eu/en/press/press-releases/2026/05/07/artificial-intelligence-council-and-parliament-agree-to-simplify-and-streamline-rules/（2026 年 5 月 26 日最終閲覧）

17 https://data.consilium.europa.eu/doc/document/ST-9247-2026-INIT/en/pdf（2026 年 5 月 26 日最終閲覧）

18 https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf（2026 年 5 月 17 日最終閲覧）

19 https://data.consilium.europa.eu/doc/document/ST-9247-2026-INIT/en/pdf（2026 年 5 月 26 日最終閲覧）

20 https://data.consilium.europa.eu/doc/document/ST-9247-2026-INIT/en/pdf（2026 年 5 月 26 日最終閲覧）

ii. AI リテラシー

EDPB 及び EDPS は、EU AI 法 4 条に基づき、AI システムの提供者及び導入者が、従業員その他関係者の AI リテラシーを十分な水準に保つための措置を講じる義務を維持すべきであると指摘しました[21]。EDPB 及び EDPS は、この義務を欧州委員会及び加盟国による奨励・支援に置き換えることは、AI リテラシー義務を大きく弱体化させ、その目的を損なうおそれがあるとしています。

5 月の暫定合意では、AI 法 4 条について、提供者及び導入者は、提供者又は導入者のために AI システムの運用又は利用に携わる従業員その他の者について、AI リテラシーの発展を支援する措置を講じるものとされています。他方で、個々人について特定の AI リテラシー水準を保証する義務ではないことも明記されています。また、欧州委員会及び加盟国は AI リテラシーの発展を支援・促進し、欧州委員会は実務上の例を公表し、AI Board は欧州の能力枠組みを考慮しつつ、共通目的の設定を含む勧告を採択するものとされています[22]。

iii. 本人の同意を欠く親密・性的コンテンツ等に関する新たな禁止

5 月の暫定合意では、AI 法 5 条の禁止 AI 実務に、本人の自由意思に基づき、特定され、十分な情報を与えられ、曖昧でなく、かつ明示的な同意なく、特定可能な自然人の親密部位又は性的に露骨な行為を描写する現実的な画像、動画、音声その他類似の素材を生成又は操作する AI システムを上市し、サービスに供し、又は利用することの禁止が追加されています[23]。児童性的虐待素材の生成又は操作に用いられる AI システムについても禁止対象とされています。

もっとも、上市又はサービス提供に関する禁止は、①当該素材の生成又は操作が AI システムの意図された目的である場合、又は、②システムの設計、訓練、アーキテクチャ、能力若しくは利用者向け機能に照らし、重要な技術的変更を要することなく、当該生成又は操作が合理的に予見可能かつ再現可能な結果であり、かつ、合理的かつ適切な技術的安全措置その他の保護措置を欠く場合に限られています。また、導入者側の禁止は、当該 AI システムがそのような素材の生成又は操作を目的として利用される場合に限定されています。これらの新たな禁止規定は、暫定合意上、2026 年 12 月 2 日から適用されるものとされています。

iv. 高リスク AI システム提供者と第三者との協力義務

5 月の暫定合意では、AI 法 25 条 4 項について、高リスク AI システムの提供者と、当該高リスク AI システムに用いられ、又は統合される AI システム、AI モデル、ツール、サービス、コンポーネント又はプロセスを供給する第三者との間で、当該提供者が AI 法上の義務を完全に遵守できるよう、一般に認められた最新技術水準に基づき、必要な情報、能力、技術的アクセスその他の支援を書面による合意で特定するものと改められています[24]。ただし、自由かつオープンソースのライセンスに基づき公衆に提供されるツール、サービス、プロセス又はコンポーネントを提供する第三者については、この義務は適用されません。もっとも、汎用 AI モデルはこの例外から除かれています。

また、暫定合意では、AI システムに変更を加えること等により新たな提供者が生じる場合について、当初の提供者の協力義務も明確化されています。この場合、当初の提供者は、当該特定 AI システムについては AI 法上の提供者とみなされなくなる一方で、新たな提供者が AI 法上の義務を履行できるよう、必要な情報、合理

---

21 https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf（2026 年 5 月 26 日最終閲覧）

22 https://data.consilium.europa.eu/doc/document/ST-9247-2026-INIT/en/pdf（2026 年 5 月 26 日最終閲覧）

23 https://data.consilium.europa.eu/doc/document/ST-9247-2026-INIT/en/pdf（2026 年 5 月 26 日最終閲覧）

24 https://data.consilium.europa.eu/doc/document/ST-9247-2026-INIT/en/pdf（2026 年 5 月 26 日最終閲覧）

的に期待される技術的アクセスその他の支援を提供するものとされています。具体的には、AI 法 16 条上の義務遵守を評価するために十分な技術文書の提供、既知の制約及び故障モードの通知、テスト及び検証のための対象を限定した技術的アクセスの提供が含まれます。ただし、当初の提供者が、当該 AI システムを高リスク AI システムに変更してはならないことを明確に指定していた場合には、この協力・文書提供義務は適用されません。

加えて、AI 法 25 条 2 項及び 4 項に基づく義務違反は、AI 法 99 条 4 項に基づく行政制裁金の対象に追加されています。この点は、第三者サプライヤーとの契約実務や、AI システムを改変・再提供する事業者の責任分担に影響し得るものです。

v. 適用時期と登録義務

5 月の暫定合意では、高リスク AI システムに関する義務の適用時期について、AI 法 6 条 2 項に基づく附属書 III 型の高リスク AI システムについては 2027 年 12 月 2 日、AI 法 6 条 1 項に基づく製品安全法制関連の高リスク AI システムについては 2028 年 8 月 2 日とされています。なお、既に上市又はサービス提供されている高リスク AI システムについては、AI 法 111 条 2 項のグレースピリオドの適用関係も明確化されています。暫定合意の前文では、少なくとも一つの個別ユニットが適用開始日前に適法に上市又はサービス提供されていた場合、同一のタイプ及びモデルの他の個別ユニットについても、設計が変更されない限り、追加的な義務、要件又は追加認証なしに、上市、提供又はサービス提供を継続できることが説明されています。他方で、適用開始日後に当該 AI システムの設計に重大な変更が加えられた場合には、高リスク AI システムに適用される関連規定を全面的に遵守する必要があります[25]。

条文上も、高リスク AI システムに関する Chapter III 及び対応する義務の適用開始日前に上市又はサービス提供された高リスク AI システムについては、当該適用開始日以降に設計上の重大な変更が加えられた場合に限り、AI 法が適用されるものとされています。ただし、公的機関による利用を意図した高リスク AI システムについては、提供者及び導入者が 2030 年 8 月 2 日までに必要な対応を行う必要があります。

また、附属書 III に掲げられる AI システムについて、提供者が AI 法 6 条 3 項に基づき高リスク AI システムに該当しないと判断する場合の EU データベース登録義務についても、暫定合意では当該登録義務を維持しつつ、登録事項を簡素化する方向が採られています。提供者は、当該判断を上市又はサービス提供前に文書化する義務を引き続き負い、当該評価は国内権限当局から要請され得るものとされています。

vi. 製品安全法制との関係及び産業 AI に関する簡素化

5 月の暫定合意では、製品安全法制の対象となる AI 組込製品について、AI 法とセクター別法制との重複を避けるための整理も行われています。まず、AI 法 6 条 1 項に基づく高リスク AI システムであって、AI 法附属書 I の Section B に掲げられる EU 調和法制の対象製品に関連するものについては、AI 法の直接適用範囲が、AI 法 6 条 1 項、60a 条及び 102 条から 112 条に限定されるものとされています。また、AI 法 57 条から 59 条についても、AI 法上の高リスク AI システム要件が当該セクター法制に統合される範囲でのみ適用される構成とされています。さらに、附属書 I の Section A に掲げられる EU 調和法制が、AI 法 9 条から 15 条及び 17 条から 25 条の要件又は義務と同等又はより高い保護水準を定める場合には、欧州委員会が 2027 年 8 月 2 日までに委任法により、AI 法上の特定の要件又は義務の適用を制限できる仕組みも設けられています。

また、AI 法上の「安全コンポーネント」の概念についても明確化が図られています。ユーザー支援、性能最適

25 https://data.consilium.europa.eu/doc/document/ST-9247-2026-INIT/en/pdf（2026 年 5 月 26 日最終閲覧）

化、サービス効率化、自動化、利便性又は安全に関係しない品質管理のみを目的とする AI システムは、安全コンポーネントに該当しないものとされています。他方で、故障又は誤作動により健康・安全が危険にさらされる AI システムは、安全コンポーネントに該当するものとされています。

特に、機械規則（Regulation (EU) 2023/1230）については、AI 法附属書 I の Section A から削除され、Section B に追加されています。これにより、機械分野については、AI 法の高リスク AI システム要件を直接適用するのではなく、機械規則側の委任法により、AI 法上の関連要件を同規則の健康・安全要件に反映させるセクター別アプローチが採られています。当該委任法は、2028 年 8 月 2 日までに適用されるものとされています。

vii. 基本権影響評価とデータ保護影響評価の関係

5 月の暫定合意では、高リスク AI システムの導入者に課される基本権影響評価（fundamental rights impact assessment。以下「FRIA」）と、GDPR35 条等に基づくデータ保護影響評価（data protection impact assessment。以下「DPIA」）との関係についても整理が行われています。AI 法 27 条上の義務の一部が DPIA により既に満たされている場合には、導入者は、FRIA において DPIA の関連箇所を相互参照し、又は DPIA の関連部分を FRIA に取り込むことができるものとされています。また、AI Office は、導入者による FRIA 義務の履行を簡素化するため、自動化ツールを含む質問票テンプレートを作成するものとされ、当該テンプレートにおいても、DPIA との相互参照又は関連部分の取込みを可能にすることが想定されています。

viii. SME・SMC に対する軽減措置

5 月の暫定合意では、SME に加え、small mid-cap enterprises（SMCs）を AI 法上の支援対象として明示する改正も含まれています。AI 法の目的規定において、イノベーション支援措置の対象として SME、スタートアップ及び SMC が明記されるほか、SME 及び SMC の定義も AI 法 3 条に追加されています。

高リスク AI システムの技術文書については、SME 及び SMC が AI 法附属書 IV に定める要素を簡易形式で提出できるものとされ、欧州委員会がそのための簡易技術文書フォームを策定するものとされています。また、品質管理システムの実装についても、SME 又は SMC である場合を含め、提供者の組織規模に比例したものとすることが明記されています。

さらに、AI 規制サンドボックスについて、AI Office が EU レベルで設置するサンドボックスでは、SME、スタートアップ及び SMC に優先的アクセスを認めるものとされています。制裁金についても、加盟国は SME、スタートアップ及び SMC の利益及び経済的存続可能性を考慮するものとされ、SME 及び SMC について一定の上限調整が設けられています。

ix. AI 規制サンドボックス及び実環境テスト

5 月の暫定合意では、AI 規制サンドボックス及び実環境テストに関する規定も見直されています。加盟国は、各国の権限ある当局が少なくとも一つの AI 規制サンドボックスを設置し、2027 年 8 月 2 日までに運用開始することを確保するものとされています。また、EDPS は EU 機関等向けに AI 規制サンドボックスを設置できるものとされ、AI Office も、AI 法 75 条 1 項の対象となる AI システムについて、EU レベルの AI 規制サンドボックスを設置できるものとされています。

AI 規制サンドボックスにおいて個人データの処理が伴う場合、又は他の国内当局の監督権限に属する事項が含まれる場合には、データ保護当局その他の関係当局が、当該事項についてサンドボックスの運用及び監督に関与するものとされています。また、サンドボックス計画には、該当する場合、実環境テスト計画を単一の文書として組み込むことができるものとされています。

さらに、暫定合意では、AI 法附属書 I の Section A に掲げられる EU 調和法制の対象となる高リスク AI システムについても、サンドボックス外での実環境テストを認める方向で規定が整備されています。附属書 I の Section B に掲げられる EU 調和法制の対象製品については、新たに AI 法 60a 条が設けられ、加盟国が実環境テストの枠組みを採用する場合には、必須の実環境テスト計画、ガバナンス及びアカウンタビリティの仕組み、並びに健康・安全及び基本権の高い保護水準を確保することが求められています。

x. AI Office の監督・執行権限及び基本権保護機関との協力

5 月の暫定合意では、AI Office の監督・執行権限についても詳細な規定が追加されています。AI Office は、一定の例外を除き、汎用 AI モデルに基づく AI システムであって、当該モデル及びシステムが同一の提供者又は同一企業グループに属する提供者により開発されたもの、並びにデジタルサービス法上の超大規模オンラインプラットフォーム又は超大規模オンライン検索エンジンを構成し、又はこれに統合される AI システムについて、AI 法上の義務の監督・執行に関する専属的権限を有するものとされています。

AI Office の所管対象となる高リスク AI システムについては、重大インシデントの報告先が AI Office とされるほか、第三者適合性評価を要する場合には、欧州委員会が上市前の適合性評価及びテストについて責任を負うものとされています。また、AI Office には、市場監視当局に相当する権限に加え、情報提供要求、遠隔又は現地検査、AI システムへのアクセス及び説明の提供命令、関連データ・文書の保存命令、拘束的コミットメント、制裁金及び日次制裁金に関する権限が付与されています。

さらに、基本権保護を所管する国内公的機関等と市場監視当局との協力関係も明確化されています。基本権保護機関は、その任務遂行に必要な場合、市場監視当局が保有又は管理する情報・文書へのアクセスを求めることができ、市場監視当局と基本権保護機関は、相互に協力し、必要な支援を提供するものとされています。

（2） 汎用 AI 行動規範署名者タスクフォースの設立

2026 年 2 月 12 日、欧州委員会は、汎用 AI（GPAI）行動規範の署名者が同年 1 月 30 日に初回の設立会合を開催し、「汎用 AI 行動規範署名者タスクフォース」（Signatory Taskforce of the General-Purpose AI Code of Practice）を設置したと発表しました[26]。同タスクフォースは、欧州 AI オフィス（AI Office）が議長を務め、参加する署名者に対し、同行動規範の実施に関連する意見交換の場を提供することで、同行動規範の一貫した適用を促進することを目的としています。また、同タスクフォースは、AI Office に義務付けられた公開協議を損なわない形で、ガイダンス文書に対して意見を提供することができます。

（3） アイスランド

2025 年 11 月 24 日、アイスランドのデータ保護当局（Persónuvernd）は、AI（人工知能）とデータ保護法の要件に関するガイダンス/解説を公表しました[27]。ガイダンス/解説の主なポイントは以下の通りです。

・ データ管理者は、AI ソリューションを含むあらゆるソフトウェアソリューションを導入する際には、以下のデータ保

[26] https://digital-strategy.ec.europa.eu/en/news/first-meeting-signatory-taskforce-general-purpose-ai-code-practice（2026 年 5 月 26 日最終閲覧）

[27] https://island.is/s/personuvernd/frett/gervigreind-og-kroefur-personuverndarlaga（2026 年 5 月 26 日最終閲覧）

護法上の要件を考慮する必要がある

- データ保護法に基づくデータ保護影響評価（DPIA）の実施要件、並びにリスク・セキュリティ評価の実施
- プライバシー通知の更新の必要性
- データ主体への情報提供

保護当局は、AI モデルに関する EDPB の 2024 年 12 月の意見や、EU におけるデジタル技術関連法制の動向にも言及している点も注目されます。

5. ヨーロッパのデータ保護規制の動向

Q5. ヨーロッパのデータ保護に対する規制動向を教えてください。

2026 年 1 月 26 日、欧州委員会は、ブラジルに対する十分性認定（Implementing Decision (EU) 2026/179）を採択しました。同日、ブラジル国家データ保護局（ANPD）も Resolution CD/ANPD No. 32/2026 を採択し、EU が LGPD と整合する保護水準を備えると認定しました。両決定は 2026 年 1 月 27 日に共同で発表され、これにより EU・ブラジル間で追加の移転措置なしに個人データの双方向の移転が可能となりました。

6. 未成年者の SNS 利用禁止

Q6. オーストラリアで導入された SNS 利用に関する最低年齢枠組みの制度概要を教えてください。

『オンライン安全改正（ソーシャルメディア最低年齢）法 2024』に基づく一定のソーシャルメディア・プラットフォームにおける 16 歳未満のアカウント保有制限が、2025 年 12 月 10 日から施行されました。同改正法は 2024 年 12 月 10 日に Royal Assent を受け、Online Safety Act 2021 に Part 4A（Social Media Minimum Age：SMMA）を新設したものです。Part 4A 自体は 2024 年 12 月 11 日に開始していますが、規制対象プラットフォーム提供者に対し、16 歳未満の対象ユーザーがアカウントを保有しないよう合理的措置を講じる義務は、2025 年 12 月 10 日から適用されました。

オーストラリアは、近年増加する若年層のソーシャルメディア利用に伴ういじめ、依存、心身への悪影響などのリスクを重く受け止め、オンライン被害の防止と健全な発育環境の確保を目的に、世界初とされる、一定のソーシャルメディア・プラットフォームにおける 16 歳未満のアカウント保有を制限する制度を導入しました[28]。本件措置は、オーストラリア国内プラットフォームだけでなく、オーストラリア国内のエンドユーザーからコンテンツにアクセスできる、又は当該ユーザーにコンテンツを配信する海外プラットフォームにも適用されます。対象となるプラットフォーム提供者は、オーストラリアに通常居住する 16 歳未満の子どもがアカウントを保有しないよう合理的な措置を講じる義務を負います。保護者の同意がある場合でも、本件措置の年齢制限は解除されません。

法令の所管は豪州インフラ・運輸・地域開発・通信・スポーツ・芸術省であり、SMMA 枠組みの実施・執行を担う規制当局はオンライン・セーフティ委員会（eSafety Commissioner）です。eSafety Commissioner は、2026 年 1 月 9 日、Grok を利用した性的コンテンツ生成への懸念を X に伝え、生成 AI サービスの安全性を重点課題と位置付けています[29]。また、2026 年 3 月 24 日には、AI コンパニオンが児童を性的に露骨なコンテンツ等にさらすリスクに関する透明性報告を公表

---

28 https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-minimum-age（2026 年 5 月 26 日最終閲覧）

29 https://www.esafety.gov.au/newsroom/media-releases/esafety-raises-concerns-about-misuse-of-grok-to-generate-sexualised-content（2026 年 5 月 26 日最終閲覧）

し、年齢確認・安全措置の不足を指摘しました[30]。

（1） 年齢制限対象ソーシャルメディアプラットフォーム

当該制限が適用される「年齢制限対象ソーシャルメディアプラットフォーム」（以下「規制対象プラットフォーム」）は、以下の全条件を充足するサービスに限られています。

- 2 人以上のエンドユーザー間の社会的交流を可能とすることが、当該プラットフォームの「唯一の」又は「重要な」目的であること
- 当該プラットフォームがエンドユーザー間のつながり又は交流を可能とすること
- 当該プラットフォームがエンドユーザーによるサービス上でのコンテンツ公開を可能とすること
- 当該プラットフォーム上のコンテンツがオーストラリア国内のエンドユーザーからアクセスできること、又はオーストラリア国内のエンドユーザーに向けて配信されていること
- 当該プラットフォームが、ユーザーの関心や行動履歴等に基づいて投稿、動画、アカウント等を自動的に推薦・表示する機能（いわゆる「おすすめ」表示機能）、またはエンドレスフィード、フィードバック機能、時間制限付きコンテンツ機能等の一定のログイン時機能を有すること

特定のプラットフォームの主要な目的が、エンドユーザー間のオンラインの社交的交流を促進するものであるかどうかの評価は、プラットフォームの具体的な機能と、それらの機能がユーザーの関与・行動・体験をどのように促進するかに依拠するものとされています。たとえば、eSafety コミッショナーは、YouTube Kids は他のプラットフォームに見られる特定の対話機能を備えていないため、規制対象プラットフォームとして分類されないことを示唆しています。

（2） 本件措置の対象外のサービス

メッセージングやオンラインゲームが主機能のプラットフォームは、本件措置の対象外であると明確に定められています。同様に、主にビジネス交流を目的とするプラットフォームも本件措置の対象外とされています。例えば、eSafety コミッショナーは暫定的に、WhatsApp はメッセージング・メール・音声/ビデオ通話による通信を主サービスとするため対象外のサービスに該当すると判断しています。

（3） 義務

規制対象プラットフォームの提供者は、16 歳未満のユーザーがアカウントを保有することを防止するための合理的な措置を講じる義務を負います。eSafety の FAQ では、合理的措置として、既存アカウントを含め、16 歳未満の対象ユーザーが保有するアカウントを発見し、削除または無効化することが期待されると説明されています。この義務の履行に伴う年齢保証の方法は法令上特定されておらず、提供者が自社で実施する場合も、第三者の年齢保証サービスを利用する場合もあり得ます。他方、提供者は、合理的な代替手段を提供しない限り、政府発行 ID の提出や豪州政府認定 Digital ID サービスの利用を強制することはできないと明言されている点は注意が必要です。

年齢保証のために収集された個人情報は、本人が年齢制限対象ユーザーであるかどうかを判定する目的、APP 6.2(b)～(e) に該当する場合、または本人の同意がある場合を除き、使用または開示することはできません。本人の同意は、任意で、十分な説明に基づき、現時点のもので、特定され、曖昧でないものでなければならず、容易に撤回可能である必要

30 https://www.esafety.gov.au/newsroom/media-releases/esafety-report-shows-ai-companions-are-putting-children-at-risk（2026 年 5 月 26 日最終閲覧）

があります。事前に選択された設定やオプトアウトによる同意取得は認められていません。また、SMMA 目的で収集された個人情報は、当該目的で使用又は開示された後、破棄する必要があります

規制対象プラットフォーム提供者は年齢確認手順を策定する際、関連する国際基準（例：IEEE 2089-2021「IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children（子どものための 5 つの権利原則に基づく年齢に適したデジタルサービス枠組みの標準）」）を参照することが推奨されています。

（4） 罰則

合理的なアクセス制御を実施しなかった規制対象プラットフォームの提供者は、法人に対して最大 4,950 万豪ドルの罰金を含む重大な制裁の対象となる可能性があります。なお、規制対象プラットフォームにアクセスした 16 歳未満のユーザー及びその保護者に対する罰則は設けられていません。

Q7. 国際的なオンラインプラットフォームの未成年者保護の現状を教えてください。

国際的には、プラットフォームによる未成年者保護の設計は大きく 3 類型に分類することができます。

第一に、「最低年齢＋アカウント作成・保持の制限」型です。代表例がオーストラリアで、2025 年 12 月 10 日から、年齢制限対象のソーシャルメディア・プラットフォームに対し、豪州の 16 歳未満がアカウントを作成・保持することを防ぐ合理的措置が義務付けられています。違反時の責任は基本的にプラットフォーム側に置かれ、未成年者本人・保護者への罰則は設けられていません。欧州でも同種の最低年齢・年齢確認をめぐる議論が進み、欧州議会は非立法的報告として、SNS、動画共有プラットフォーム、AI コンパニオンについて、16 歳を原則的なデジタル最低年齢、13～16 歳は保護者の同意を要する年齢とする方向の議論が政治的に提起されています。

第二に、「オンライン安全法制＋年齢確認＋安全設計・機能制限」型です。EU はデジタルサービス法（DSA）28 条で未成年が利用し得るオンライン・プラットフォームに高いレベルの安全・プライバシー・セキュリティを求めつつ、同条の遵守のために「利用者が未成年かどうかを判定するための追加の個人データ処理を義務付けない」とも明記しています。これを受け、欧州委員会は未成年者保護ガイドラインを公表し、年齢確認ソリューションのブループリント（プロトタイプ）についても加盟国との展開を進めています。

第三に、「個人情報保護（未成年者データ）の処理を中心に『禁止』ではなく『抑制』する」型です。典型が、米国連邦の COPPA（13 歳未満向けのサービス等における子どもの個人データの収集・利用・開示に検証可能な保護者のの同意を要求）や、インドの DPDP 法（18 歳未満の子どもの個人データ処理に「検証可能な保護者の同意」を要求するとともに、トラッキング・モニタリング・子ども向けターゲティング広告を制限）です。この類型は「SNS 利用そのもの禁止」ではなく「未成年者のデータ利用を絞って実害を抑える」発想に立つものです。年齢確認・保護者確認の仕組みの設計次第では実装コストやプライバシー上の摩擦が残る一方で、利用時間や依存的設計への直接的な歯止めとしては限界があるという指摘が見られます。

- 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

- 本ニュースレターの執筆者は、以下のとおりです。
  弁護士 中崎 尚（takashi.nakazaki_grp@amt-law.com）

- ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

- ニュースレターのバックナンバーは、こちらにてご覧いただけます。