年齢保証 (Assurance) に関するステートメント 1/2025

2025 年 2 月 11 日採択

欧州データ保護委員会は以下の声明を採択した：

1. 本声明の背景と目的

1. 欧州の規制枠組みは、デジタル環境における子どもの保護強化を求めている。例えば、加盟国が国内法として適用している視聴覚メディアサービス指令（Audiovisual Media Services Directive）[1] は、年齢確認措置を実施する可能性を強調している（第 6 条 a および第 28 条 b）。GDPR は、情報社会サービスの文脈におけるパーソナルデータの処理に同意するための最低年齢要件を導入しており（第 8 条）、デジタルサービス法（Digital Services Act）[2]は 、リスク緩和措置として年齢確認に言及している（第 35 条 1 項）。また、多くの加盟国が、法的行為の実行、特定の権利の行使、特定の商品やサービスへのアクセスに関する最低年齢要件を国内法に導入している。

2. 加えて、Better Internet for Kids（BIK+）のような国や欧州のさまざまなイニシアチブは、欧州のデジタル権と原則（European Digital Rights and Principles）[3] 、安全で年齢に適したデジタル環境を通じて、オンライン上の子どもの幸福を向上させるための解決策の一つとして、年齢保証 (Assurance) を挙げている。

3. 調査報告書「年齢保証の類型と要件のマッピング」（*Mapping age assurance typologies and requirements*）[4] 、その中でプロバイダが提示した定義に基づき、本文書では「年齢保証」を「個人の年齢又は年齢範囲を、様々なレベルの信頼性又は確実性をもって決定するために使用される方法の総称」として使用する。同報告書では、年齢保証の主要なカテゴリーとして、年齢推定、年齢検証、自己申告の 3 つを挙げている。

4. 年齢保証は、個人データ保護に対する自然人の権利だけでなく、無差別的権利、個人の完全性に対する権利、自由と安全に対する権利、自由な表現と情報に対する権利など、その他の権利と自由[5] にも悪影響を及ぼす可能性があり、データ保護に特有のリスクをもたらす。

---

[1]2018 年 11 月 14 日付欧州議会および理事会指令（EU）2018/1808 は、市場の現実の変化に鑑み、視聴覚メディアサービスの提供に関する加盟国の法律、規則または行政措置により定められた一定の規定の調整に関する指令 2010/13/EU（視聴覚メディアサービス指令）を改正するものである（https://eurlex.europa.eu/eli/dir/2018/1808/oj）。

[2]デジタルサービスの単一市場および指令 2000/31/EC の改正に関する 2022 年 10 月 19 日付欧州議会および理事会規則（EU）2022/2065（デジタルサービス法） , https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[3]Better Internet for Kids、年齢保証ガイド、 https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest

[4]Raiz Shaffique, M., & van der Hof, S. (2024).年齢保証の類型と要件のマッピング。European Schoolnet (EUN)がコーディネートし、欧州委員会が委託した Better Internet for Kids (BIK)プロジェクトの一部である。

[5]年齢確認が権利と自由に与える潜在的な影響については、以下を参照のこと：「年齢検証のためのロードマップ」（オーストラリア eSafety）を参照のこと。Commissionner, 2023） https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-backgroundreport.pdf?v=1731644498261, "A safe internet by default for children and role of age verification" （AEPD, 2024） https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf or "Trustworthy Age

5. 年齢保証に関する EU レベルでの一貫したアプローチの重要性を認識し、EDPB は、年齢保証の文脈でパーソナルデータの処理が行われる際に考慮されるべき、GDPR に由来する具体的なガイダンスとハイレベルの原則を提供したい。

6. この保護原則は、年齢保証の観点から、子どもの保護と個人データの保護を両立させようとするものである。

7. GDPR 第 5 条に記載されている主要原則（適法性、公平性、透明性、目的の限定、データの最小化、正確性、保存の制限、機密性、完全性、説明責任）に関する要件に優先的に対応し、GDPR 第 25 条「設計およびデフォルトによるデータ保護」および GDPR 第 32 条「処理のセキュリティ」で規定されているように、これらのデータ保護原則が適切に実施され、長期にわたって堅固であり続けることを保証する。

8. 本声明は、商品の購入、子どもに危害を及ぼす可能性のあるサービスの利用、または法的行為の実行について、適用法またはその他の方法で最低年齢が定められている場合、および子どもを保護する注意義務がある場合（たとえば、サービスが年齢に適した方法で設計または提供されていることを保証する場合）を含む、さまざまなオンライン利用ケースに適用される原則に焦点を当てている。

9. EDPB はまた、関連する都度、他の文書において、特定のユースケースに関する追加ガイダンスを発行することを検討してもよい。

2. GDPR に準拠した年齢保証を設計するための原則

2.1 権利と自由を完全かつ効果的に享受する

10. 年齢保証は、自然人の基本的権利（[6]）および自由を全面的に尊重しなければならず、プロセスに関わるすべての当事者にとって、子どもの最善の利益が第一に考慮されるべきである。

11. 年齢保証を実施する場合、プロバイダは個人データ保護の権利だけでなく、自然人のすべての基本的権利への影響も考慮するようにすべきである。

12. 具体的な子どもの場合、子どもの最善の利益（[7]）は、年齢保証に関わるすべての当事者にとって第一に考慮されるべきものである。子どもの最善の利益を考慮する上で、上下関係がないことに留意することが重要であ

Assurance?" a study commissioned by Greens/EFA Cluster on Green and Social Economy at European Parliament（2024） https://www.greensefa.eu/en/article/document/trustworthy-age-assurance

[6]特に、世界人権宣言、欧州人権条約、欧州連合基本権憲章、国連子どもの権利条約である。

[7]国連子どもの権利委員会は、最善の利益の原則が「条約で認められているすべての権利の完全かつ効果的な享受と、子どもの全人的な発達の両方を確保することを目的としている」ことを明らかにしている。子どもの最善の利益が第一義的に考慮される権利（第 3 条第 1 項）に関する一般的意見第 14 号（2013 年）、https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC C GC 14 ENG.pdf

り、個人データの保護、暴力およびその他あらゆる形態の搾取からの保護、さまざまな情報源からの情報へのアクセス、およびその意見が正当な重みを持って考慮される権利など、すべての子どもの権利（[8]）に配慮すべきである。

2.2 年齢保証の比例性に関するリスクベースのアセスメント

13. 年齢保証は常に、自然人の権利と自由に適合するような、リスクベースかつ比例的な方法で実施されるべきである。

14. プロバイダは、サービスを設計・運営する際、リスクに基づいたアプローチを採用すべきである。年齢保証のような安全対策を用いる必要性と比例性は、関連するリスク を考慮して実証されるべきである。その必要性は、有害な接触やコンテンツへのエクスポージャーな ど、特定のサービスが子ども（[9]）にもたらすリスクを特定し評価するために、アセスメント（[10]）を実施することで証明することができる。このアセスメントの一環として、プロバイダは、年齢に応じた参加を確保するために、子どもの権利、デジタル環境が提供する機会、子どもの意見、子どもの能力の発達も考慮することができる 。[11]

15. サービスプロバイダーはまた、個人データ保護の権利を含むユーザーの権利と自由を尊重し、利用可能なもののうち常に最小限の侵入であるべきであり、常に効果的であるべき安全対策の必要性とのバランスを取らなければならない。多くの場合、年齢保証はデータ対象者の権利と自由に高いリスクをもたらすため、処理の前に、処理の性質、範囲、文脈および目的を考慮して、データ保護影響アセスメント（「DPIA」、GDPR 第 35 条）を実施する必要がある。DPIA は、想定される処理業務および処理の目的（該当する場合、管理者が追求する正当な利益を含む）の体系的な説明を含むべきである。また、処理の必要性と比例性のアセスメントを含み、年齢保証を目的としたパーソナルデータの処理から生じるリスクを特定し、それらのリスクを緩和するための手段を含むべきである（[12]）。

16. DPIA は、データ保護遵守のための適切な技術的・組織的措置の設計と実施の指針となるべきである。このようなリスク・ベースのアプローチは、自然人の権利と自由に対する潜在的な干渉と、この特定の状況における意図された目的、すなわち子どもの安全とのバランスをとる際に極めて重要である。権利と自由への影響という観点から、この干渉の範囲、程度、強度を常に注意深く評価しなければならない[13]。例えば、サービス・プロバイダが

---

[8]デジタル環境に関する子どもの権利に関する一般的意見第 25 号（2021 年）、OHCHR、2021 年 3 月

[9]子どもの権利分野の専門家は、子どもの権利インパクト・アセスメント（CRIA）を「条約（子どもの権利）とその第 3 条（子どもの最善の利益を優先させること）を、具体的かつ構造的な方法で実践に移す」ための効果的なツールとして活用することの利点を強調している（Mukherjee, S., Pothong, K., & Livingstone, S. (2021).子どもの権利インパクト・アセスメント：デジタル環境において子どもの権利を実現するためのツール。London: 5Rights Foundation）。 さらに国連委員会は、デジタル環境の規制と設計に子どもの権利を組み込むため、CRIA の利用を義務付けるよう各国に求めている

[10]例えば、子どもの権利影響アセスメント（「CRIA」）は、DPIA の一部である場合もあれば、そうでない場合もある。

[11]デジタル環境に関する子どもの権利に関する一般的意見第 25 号（2021 年）、OHCHR、2021 年 3 月。

[12]データ保護影響アセスメント（DPIA）に関する EDPB ガイドラインおよび規則 2016/679 の目的上、処理が「高リスクになる可能性が高い」かどうかの判断 https://ec.europa.eu/newsroom/article29/items/611236/en

[13]プライバシーおよび個人データ保護に対する基本的権利を制限する措置の比例性評価に関する EDPS ガイドライン https://www.edps.europa.eu/sites/default/files/publication/19-02-25 比例性ガイドライン ja.pdf

すべてのコンテンツやサービスにアクセスする際に、すべての利用者の年齢を確認するためにパーソナルデータの処理を行うことは、そのコンテンツやサービスがすべての利用者に適しており、リスクがない場合であっても、必要性と比例性のテストには合格しない。

2.3 データ保護リスクの予防

17. 年齢保証は、個人にとって不必要なデータ保護リスクにつながるものであってはならない。特に、年齢保証は、サービス・プロバイダが自然人を識別、特定、プロファイリング、追跡するための新たな手段を提供すべきではない。

18. サービス・プロバイダおよび年齢保証に関与する第三者は、このプロセスが、 自然人の識別、位置特定、プロファイリング、または追跡から生じるような不必要 なデータ保護リスクを引き起こさないように、効果的な対策および保護措置を講じるべきである。年齢保証のためのパーソナルデータの処理は、年齢保証自体とは無関係な目的を 達成するための追加的手段を提供すべきではない。そのためには、設計およびデフォルトによるデータ保護の原則（第 2.8 節参照）に完全に準拠した年齢保証のアプローチを選択し、データ対象者に不当な不利益、違法な差別、予期せぬ、または誤解を招くような方法で個人データが処理されないことを保証する、公正性の原則を保証する措置を実施することが必要である。

19. たとえば、アダルト・コンテンツにアクセスするために年齢を確認する必要がある自然人は、サービス・プロバイダが年齢保証を使用して身元または正確な地理的位置を決定したり、身元に関する個人的側面を監視、評価または推論したりすることを 期待しないであろう。この事実は、公平性、透明性、目的の限定を含む第 5 条 1 項のデータ保護の原則、および個人データのその後の利用に関する第 6 条 4 項の規則の遵守に特に関連する。同様に、第 5 条 1 項の目的限定とデータ最小化の原則に従い、年齢保証プロセスは、商業的（例：パーソナライズされた広告）および悪意のあるターゲティング（例：グルーミング、いじめ、ストーキングまたは嫌がらせ）の両方を含む、利用者のさらなるターゲティングまたはプロファイリングを可能にしてはならない。EDPB は、前文に基づき、個人データが脆弱な自然人、特に子どもに関連する場合、データ保護権に特別なリスクが生じる可能性があることを想起する。一般的に、年齢保証プロセスで使用される情報に基づくプロファイリングによって、自然人およびその行動について必要以上に知ることはできないはずである。このことは、データ侵害が発生した場合にも、可能な限り確保されなければならない。

20. サービス・プロバイダが、代理権がないために個人を不必要なデータ保護リスクに直面 させることを防ぐために、力の不均衡状況は避けるべきである[14] 。これが不可能な場合、このような状況を認識し、適切な対応策を講じるべきである[15] 。例えば、年齢を証明するための実行可能な代替手段を、年齢を保証する特定の 方法を使用できない、または使用したくない利用者に提供すべきである。さらに、プロバイダは、サードパーティから提供された

[14]例えば、データ対象者が適切な救済措置なしに自動化された意思決定に直面する場合や、 同意が自由に与えられない場合などである。権力の不均衡」概念については、大規模オンラインプラットフォームが実施する同意または有料モ デルの文脈における妥当性確認に関する EDPB 意見書 08/2024（4.2.1.3 項）、https://www.edpb.europa.eu/system/files/202404/edpb opinion 202408 consentorpay en.pdf で議論されている。

[15]EDPB ガイドライン 03/2022「ソーシャル・メディア・プラットフォームのインターフェイスにおける欺瞞的なデザイン・パターン：どのように認識し、回避するか（セクション 2.3）」バージョン 2.0 より https://www.edpb.europa.eu/system/files/2023-02/edpb 03-2022 Guidelines on deceptive design patterns in social media platform interfaces v2 en 0.

ものを含め、選択された 方法および技術がその目的に沿って機能しているかどうかを定期的に評価し、処理の公 平性を確保するためにそれらを調整すべきである。また、年齢保証に関わる第三者は、不必要なデータ保護リスクを持ち込まず、方針、設計、サービスなどに関連する変更があれば適時に通知することにより、サービスプロバイダーがその義務を遵守するのを支援するよう努めるべきである。

2.4 目的の制限とデータの最小

21. サービスプロバイダーおよび年齢保証に関与するサードパーティは、その指定された、明示的かつ正当な目的のために厳密に必要な年齢関連属性のみを処理すべきである。

22. ほとんどの場合、年齢保証の目的は、年齢に関連したアクセス管理の決定、子どものオンライン上の危害の防止、年齢に応じた適切なデザインや体験の提供などである。ユースケースにかかわらず、パーソナルデータの処理目的は具体的かつ明示的でなければならない（GDPR 第 5 条 1 項 b）。一旦個人データが収集された後は、その目的とは相容れない方法でさらに処理したり、追加データと組み合わせたりしてはならない。プライバシー強化技術（「PET」）などの技術的手段を用いて、個人データの再利用の可能性を制限しなければならない。個人データの再利用を制限するポリシーや契約義務などの組織的措置（[16]）も展開すべきである。

23. 年齢関連属性とは、自然人がある年齢であること、ある年齢以上であること、ある年齢未満であること、ある年齢の範囲内であることを示す属性をいう。目的特定により、収集すべき関連する必要な年齢関連属性が決定される。これを行うことで、管理者は年齢保証プロセスの比例性を評価することもできる。このプロセスから生じるメリットは、基本的権利の行使に関するデメリット[17] （上記セクション 2.2 を参照）に勝るものであってはならない

24. したがって、データ管理者は、提供しようとする目的に対して必要かつ適切で、関連性のある個人データのみを収集すべきである。このように、データの最小化は、必要性（[18]）と比例性の原則を実証し、運用するのに役立つ。例えば、サービス・プロバイダは、ユーザーがある年齢閾値以上か以下かを知ることだけが必要な場合がある。これは、サードパーティ・プロバイダの参加に基づくトークン化されたアプロ ーチによって実施することができ、その場合、サービス・プロバイダは年齢保証プロセスの機能結果（例 えば、年齢閾値を「超える」か「下回る」か）のみを見ることができる（[19]）。サービス・プロバイダが、ユーザが特定の年齢の範囲内にあるか、または特定の年に生まれたかどうかを知る必要がある場合、異なるアプローチが関連する可能性がある。

---

[16] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb ガイドライン 201904 dataprotection by design and by default v2.0 en.pdf（設計およびデフォルトによる第 25 条データ保護に関する EDPB ガイドライン 4/2019 バージョン 2.0）より

[17] プライバシーおよび個人データ保護に対する基本的権利を制限する措置の比例性の評価に関する EDPS ガイドラインより https://www.edps.europa.eu/sites/default/files/publication/19-02-25 比例性ガイドライン ja.pdf

[18] EDPS toolkit for Assessing necessity of measures that limit basic right to protection of personal data, https://www.edps.europa.eu/sites/default/files/publication/17-06-01 necessity toolkit final en.pdf より。

[19] サードパーティーのプロバイダが年齢チェックを行い、ユーザーに「年齢トークン」を提供する。この「年齢トークン」を提示することで、ユーザーは再度年齢を証明する必要がなく、サービスプロバイダに提示することができる。年齢トークンには、異なるユーザーの属性や、いつ、どこで、どのように年齢チェックが行われたかが含まれる場合がある。

2.5 年齢保証の効果

25. 年齢保証は、その実施目的に見合った有効性のレベルを実証的に達成しなければならない。

26. 年齢保証を実施する手段は、処理の目的を達成するために適切でなければならない。特に、法的に義務付けられた年齢保証措置の有効性は、必要性（[20]）と比例性（[21]）の原則を満たす前提条件として考慮されるべきである

27. 年齢保証の有効性は、以下のようないくつかの側面から評価されるべきである

a) アクセシビリティ：年齢保証は、自然人が年齢を確認するため、または年齢関連の要件を満たしていること を証明するために、広くアクセス可能でなければならない。あるカテゴリーに属する個人が、例えば適切な ID 文書または携帯電話を所有していない、あるいは障 害を理由として、特定の年齢保証方法によって識別的差別を受けるリスクにある場合、年齢 保証のための代替方法は、合理的に可能な場合には、適切なレベルのプライバシー、 安全性およびセキュリティを伴って利用可能にされるべきである。年齢保証ソリューションは、アクセシビリティ（[22]）に関するあらゆる適用法にも準拠すべきである。

b) 信頼性：正確性の原則（GDPR 第 5 条(d)）によれば、自然人が年齢に関連する要件を満たすか否かを判断することを目的とするあらゆる方法は、当該要件を満たすか否かを判断する際に、適切かつ一貫したレベルの正確性を提供すべきである。特に、年齢に関する属性が適切に確立されていない場合など、自動化された意思決定によって利用者が大きな影響を受ける可能性がある場合には、適切な救済メカニズムが利用できるようにすべきである（下記 2.7 項参照）。

c) 堅牢性：年齢保証は、予期せぬ状況に対処でき、システムを騙したり迂回したりする合理的な可能 性のある試みに抵抗できなければならない。年齢関連属性の自己宣言の文脈では、頑健性はほとんど意味を持たないことに留意すべきであ る。なぜなら、そのような方法の信頼性は、ほとんど利用者の善意に依存するからである[23]。

加えて、年齢保証を実施するプロバイダ及びプロセスに関与するサードパーティは、その 有効性を実証し、適切なレベルのアクセシビリティ、信頼性及び堅牢性に到達する手段について透明 性を持たなければならない（2.10 節参照）。

---

[20]EDPS toolkit for Assessing the necessity of measures that limit basic right to protection of personal data, https://www.edps.europa.eu/sites/default/files/publication/17-06-01 necessity toolkit final en.pdf 個人データ保護の基本的権利を制限する措置の必要性をアセスメントするための EDPS ツールキット。

[21]プライバシーおよび個人データ保護に対する基本的権利を制限する措置の比例性評価に関するガイドライン https://www.edps.europa.eu/sites/default/files/publication/19-02-25 比例性ガイドライン ja.pdf

[22]例えば、公共部門のウェブサイトやモバイルアプリケーションのアクセシビリティや、製品やサービスのアクセシビリティは、それぞれウェブアクセシビリティ指令（WAD）や欧州アクセシビリティ法（EAA）によってプロバイダが規定されている。年齢保証ソリューションは、ICT 製品とサービスのアクセシビリティ要件に関する欧州標準規格 EN 301 549 v3.2.1 の要件を満たすことで、これらの法規制に適合していることを確認しなければならない。

[23]EDPB は以前、TikTok Technology Limited に関してアイルランドの SA から提出された紛争に関する拘束力のある決定書 2/2023 において、高リスク処理の文脈における年齢検証方法としての自己申告の有効性に重大な疑念を表明している。(Art. 65 GDPR), https://www.edpb.europa.eu/system/files/2023-09/edpb bindingdecision 202302 ie sa ttl children en.pdf

2.6　合法性、公平性、透明性

28. サービスプロバイダーおよび年齢保証に関与するサードパーティは、年齢保証を目的としたパーソナルデータの処理が、適法かつ公正で、利用者に対して透明性のあるものであることを保証すべきである。

29. プロバイダは、年齢保証の文脈でパーソナルデータの処理を行うために、GDPR 第 6 条（および関連する場合は第 9 条 2 項に規定された適用例外）に基づく適用可能な法的根拠があることを確認しなければならない。例えば、法的義務（GDPR 第 6 条(1)(c)）を遵守するために年齢保証を展開する必要がある場合があり、年齢保証は追求される正当な目的および GDPR 第 6 条(3)に規定される要件に釣り合うものでなければならないことを考慮しなければならない。

30. さらに、プロバイダは、個人データが具体的に誰にどのように利用されるのかについて、利用者に透明でなければならない。これは、年齢保証プロセスに複数の関係者が関与している場合に特に重要である。年齢保証の目的で個人データが処理される前に、利用者は（GDPR 第 12 条、第 13 条および第 14 条に従って）特に[24]：

- どのような個人データがどのように処理されるのか；
- サードパーティがプロセスに関与するかどうか、関与する場合はそのサードパーティは誰か、またこのシナリオにおける管理者と処理者は誰か；
- 自分のデータが他者と共有される場合、または第三国に転送される場合
- 個人データの保存期間、またはそれが不可能な場合は保存期間を決定する規準
- 年齢保証の結果下された誤った決定に異議を唱える方法を含め、個人データに関する個人の権利とは何か（GDPR 第 15 条から第 22 条）。

31. 年齢保証における透明性は、子どもに関して特に重要である。プロバイダは、関係する場合、透明性に関する情報を、子どもにとって明確で理解しやすい方法で伝えるようにしなければならない。

32. 透明性の概念は、基本的に公平性と関連している。もしプロバイダが、年齢保証のために自然人の情報をどのように処理しているのかについて明確かつ透明でない場合、この処理が公正であるとみなされる可能性は低く、ひいてはこの処理が合法である可能性も低くなる。特に、プロバイダが利用者の年齢を確認するために様々な方法を提供する場合、データ保護の観点からそれぞれの方法が持つ影響について透明性を確保すべきである。

[24]規則 2016/679 に基づく透明性に関する第 29 条作業部会ガイドライン（https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_ja.）を参照のこと。

2.7　自動意思決定

33. 年齢保証の文脈で自動意思決定が行われる場合は、GDPR を遵守すべきである。該当する場合、サービスプロバイダーおよび関係するサードパーティは、自然人の権利と自由および正当な利益を保護するための適切な措置を提供すべきである。

34. EU の立法者は、自動化された意思決定の広範な定義を選択し、ケースバイケースで検討することを求めている[25]。自動化された意思決定は、コンテンツやサービスにアクセスするため、あるいは年齢を証明するために展開される方法を通じて、年齢保証プロセスのさまざまなステージで関与することができる。

35. 完全に自動化された年齢保証は、関係する自然人に対して、例えば表現の自由の行使に対す る法的効果を生じさせるか、あるいは少なくとも、同様の方法でに重大な影響を与える可能性がある[26]。自動化された年齢保証が自然人の権利に及ぼす影響は、関係するコンテンツやサービスの種類に よって異なる可能性がある。

36. 従って、サービス・プロバイダおよび年齢保証に関与するサード・パーティは、 年齢に関連する属性が適切に確立されていない利用者に対して、救済策および適切な賠 償メカニズムを提供しなければならない。年齢保証プロセスのアーキテクチャーによっては、データ対象者がその権利 を行使するために誰に連絡すべきかを特定しなければならない[27]。

37. サービスプロバイダや関係するサードパーティは、子どもが関係する場合には特に注意を払うべきである。GDPR の前文 71 に記載されているように、「法的またはそれに準ずる重大な影響を伴う［……］、もっぱら自動化された意思決定は、［……］子どもに関するものであってはならない」。このルールの例外は、「子どもの福祉を保護するために」必要な場合など、限られた状況下で残されるべきである[28]。いかなる場合においても、サービスプロバイダーおよび関係するサードパーティは、適切な手段、例えば、実行可能な代替手段、救済メカニズム、場合によっては人的介入を、関係する場合には、子どもに適合した情報とともに実施すべきである。

---

[25]C-634/21、シュファ・ホールディング事件（採点）：2023 年 12 月 7 日付裁判所（第一審）判決（Verwaltungsgericht Wiesbaden - Germany からの予備判決請求） - OQ v Land Hessen（予備判決請求-パーソナルデータの処理に関する自然人の保護-規則（EU）2016/679-第 22 条-自動化された個人の意思決定-信用情報機関-将来における支払約束を履行する能力に関する確率値の自動的設定（「スコアリング」）-第三者による当該確率値の使用）, https://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=CELEX%3A62021CA0634

[26]規則 2016/679 を目的とした自動化された個人の意思決定とプロファイリングに関するガイドライン https://ec.europa.eu/newsroom/article29/items/612053/en

[27]EDPB のガイドライン（前述）に記載されている通りである：これらの権利は、プロファイルを作成する管理者と、データ対象者について（人の介在の有無にかかわらず）自動化された決定を行う管理者に対して、これらの事業体が同一でない場合には、訴えられる」。

[28]規則 2016/679 の目的における個人の自動意思決定とプロファイリングに関するガイドラインより：「それにもかかわらず、管理者が、例えば子どもの福祉を保護するためなど、子どもとの関係において、法的またはそれに準ずる重大な効果を有する、プロファイリングを含む、もっぱら自動化された意思決定を実施することが必要な状況が存在する可能性がある。

2.8 設計とデフォルトによるデータ保護

38. 年齢保証は、GDPR の要件を満たし、データ対象者の権利を効果的に保護するために、利用可能な最もプライバシーを保護する方法および技術を考慮して設計、実施、評価されるべきである。

39. GDPR 第 25 条に基づき、年齢保証に関与するデータ管理者は、すべてのデータ保護の原則、ひいてはデータ対象者の権利と自由を効果的に履行するために、適切な技術的・組織的措置および必要な保護措置を実施すべきである。パーソナルデータの処理活動の設計段階において、デフォルトでデータ保護を考慮に入れるというデータ管理者の要件は、処理者、および処理ライフサイクル全体にも適用される。

40. 年齢保証システムに関連するリスクの多様性と重大性を考慮し、特に ID 文書または生体データ などの特殊カテゴリの個人データが処理される場合は、個人データへの不必要なアクセス、処理、 共有、および保管を回避するために最大限の注意を払うべきである。年齢保証システムおよびそのようなシステムの要件を規定する法的または技術的な文書も、デジ タル ID 管理の分野におけるプライバシー強化技術の急速に変化する状況を考慮に入れて、必 要に応じて定期的に改訂および更新されなければならない。

41. EDPB guidelines on data protection by design and by default[29] で言及されているように、GDPR 第 25 条の文脈における「最新技術（state of the art）」という言及は、前述の適切な技術的・組織的措置を決定する際に、市場で利用可能な技術の現在の進歩を考慮する義務をデータ管理者に課している。標準、ベストプラクティス、および関連する利害関係者によって認識されている行動規範は、そのような措置を決定する際に役立つ。ただし、これらの措置の適切性は、特定の処理活動ごとに検証されなければならない。

42. その結果、EDPB は、本文書が作成された時点における年齢保証の技術状況に基づき、ユーザー保有データおよび安全なローカル処理（デバイスベース）を支持し、リンク不能性[30] （異なる当事者から見た場合、および結託や個人データ漏えい の場合でも）などの特性や、データ対象者の管理下にあるパーソナルデータの選択的開示[31] を可能にする技術およびアーキテクチャーに十分な配慮を行うことを推奨する。さらに、シングルユース・クレデンシャルのバッチ発行[32] やゼロ知識証明[33] のような暗号プロトコルに依存するようなアプローチの使用は、年齢保証がデータ対象者のプライバシーに高いリスクを伴う可能性がある場合には、データ対象者が利用できるようにすべきである。

---

[29]EDPB ガイドライン 4/2019 第 25 条「設計による、およびデフォルトによるデータ保護」バージョン 2.0, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb ガイドライン 201904 dataprotection by design and by default v2.0 en.pdf

[30]非好感度特性は、異なるデータ項目、アクション、トランザクションを特定のデータ対象者に関連付けたり、相関させたりすることが不可能であることを意味する。

[31]選択的開示は、トークン、クレデンシャル、および認証の機能であり、データ対象者がケース・バイ・ ケースで特定の当事者と希望する情報のみを共有することを可能にする。

[32]バッチ発行は、データ対象者からの 1 つのクレデンシャル要求に、同時に生成されたクレデンシャ ルのセットまたはグループで対応することに依存する。

[33]ゼロ知識証明とは、一方の当事者（証明者）が他方の当事者（検証者）に対して、与えられた文が真であることを、その文が真であるという単なる事実以上の情報を伝達することなく証明できるプロトコルのことである。

2.9　年齢保証

43. サービスプロバイダーおよび年齢保証に関わるサードパーティは、リスクに見合ったセキュリティレベルを確保するために、適切な技術的・組織的対策を実施すべきである。

44. GDPR は、管理者と処理者の双方に、処理される個人データのリスクに見合ったセキュリティレベルを確保するための適切な技術的・組織的措置を講じることを求めている（前文 83 および第 32 条）。年齢保証に関わる個人データの性質、機密性、量は、データ漏えいがもたらす潜在的な悪影響を浮き彫りにしている。

45. 信頼モデルは、異なる当事者が互いのアイデンティティと完全性をどのように検証するかを定義するため、年齢保証の文脈におけるデータ漏洩を防ぐために極めて重要である。信頼モデルは、事前に関係を持たない参加者間の安全なコミュニケーションとデータ交換を促進する。加えて、個人データの仮名化と暗号化は、データ漏えいの起こりうる悪影響を緩和するために有用な手段である。保存制限の原則を満たし、短い保存期間を使用することも、年齢保証におけるセキュリティには不可欠であり、エクスポージャーを減らすことができる。ユーザーの年齢が確認されると、年齢保証プロセスに使用された個人データの記録は残らない。

46. 実際には、年齢保証の実施に対する法的圧力の高まりと、そのような規則の対象となりうるプロバイダの数を考えれば、セキュリティ侵害の発生は予想されるはずである。[34]情報漏えいが発生したかどうかを即座に確認するために、適切な技術的保護と組織的措置がすべて整備されているかどうかを確認する必要がある。データセキュリティポリシーの重要な要素は、可能な限り情報漏えいを防止し、情報漏えいが 発生した場合にはタイムリーに対応できることである。したがって、セキュリティ侵害後、年齢保証の可用性を速やかに回復する能力も不可欠であると考えるべきである。同様に、年齢保証のエコシステムのレジリエンスを確保することは極めて重要であり、異なる選択肢の存在を支持し、緩やかに結合された関係者（[35]）は、一つの障害や故障が重大なアクセス制限を引き起こすほど互いに依存しない。

47. セキュリティ対策は年齢保証において最も重要であるが、個人データへの権限のあるアクセスまたは権限のないアクセスが自然人の権利に影響を与えないことを保証するものではない。セキュリティ対策は、必要性、比例性、またはデザインおよびデフォルトによるデータ保護の原則の適用に取って代わることはできない。

2.10 説明責任

48. サービスプロバイダーおよび関係するサードパーティは、年齢保証へのアプローチ、およびデータ保護規制およびその他の法的要件への準拠を実証するための説明責任を果たすことができるガバナンス手法を導入すべきである。

49. 様々な利害関係者の関与を考えると、年齢保証ガバナンスはその説明責任において重要な 役割を果たす。年齢保証はガバナンスの枠組みのもとで運営されるべきであり、すべてのプロセスとシス テムがデータ保護規制とそ

[34]GDPR における個人データ漏えい通知に関する EDPB ガイドライン 9/2022 より
https://www.edpb.europa.eu/system/files/202304/edpb ガイドライン 202209 個人データ漏えい通知 v2.0 ja.pdf

[35]当事者は可能な限り互いに依存し合うことで、変化や障害が発生したときの影響範囲を小さくする。

の他の法的要件を満たす方法で設計、実施、改訂、文書化、防御、 使用、維持、テストまたは監査されることを保証する。この枠組みには、少なくとも、データ保護方針（GDPR 24 条 2 項）、コンプライアンス目標を達成し、年齢保証のライフサイクル全体にわたってリスクを適切に管理するために必要な優先順位付けと意思決定プロセスが含まれるべきである。

50. 例えば、ガバナンスの枠組みは、管理者／被処理者の観点から、処理の中のどの正確な活動又は業務について、誰がどのように責任を負うかを明確にすべきである。また、年齢保証が当局や関連利害関係者によって効果的に監査可能であることも保証されなければならない。ガバナンスの枠組みは、説明責任だけでなく、年齢保証の透明性と信頼性にも不可欠である。データ対象者は、運用や意思決定などについて透明性のある方法を信頼する可能性が高い。

51. さらに、ガバナンスの枠組みの一部として、年齢保証の有効性（2.5 項）、設計およびデフォルトによるデータ保護（2.8 項）、セキュリティ（2.9 項）の確保が含まれる。

欧州データ保護委員会のために
議長
(アヌ・タラス)

採択

採択