ガイドライン

ガイドライン 3/2025

DSA と GDPR の相互関係に関するガイドライン

バージョン 1.0

2025 年 9 月 11 日採択

採択済み - 公開協議用バージョン

エグゼクティブサマリー

デジタルサービス法（DSA）は、仲介サービスプロバイダに対する様々な規則と義務を定めている。DSA はDSA に基づく管轄当局、欧州デジタルサービス委員会（EBDS）、EU 裁判所による解釈の対象となるが、GDPR における「プロファイリング」や「特別な種類のデータ」に言及する規則など、データ保護の法的枠組みに関連する複数の規定があり、仲介サービスプロバイダーによるパーソナルデータの処理に影響を及ぼす。

各規制に基づく監督当局による DSA と GDPR の一貫した解釈・適用、およびこの整合性を確保する適切なメカニズムは、仲介サービスプロバイダへの法的確実性を提供し、最終的にデータ対象者の権利と自由を防御する上で重要である。

本ガイドラインは、DSA の規定の一部が仲介サービスプロバイダーによるパーソナルデータの処理に関わり、GDPR の概念や定義を参照している点において、DSA と GDPR の一貫した解釈・適用に寄与することを目的とする。本ガイドラインは、GDPR との重要な相互作用が認められる DSA の特定規定に焦点を当てる。

本ガイドラインは、DSA 第 7 条に基づく違法コンテンツの検知、識別、対処（例：収益化の停止、削除、アクセス無効化）の取り組みが、様々な技術を用いたパーソナルデータの処理を伴う可能性があることを認識している。コンテンツモデレーションの文脈で緩和すべき個人への特定リスクを強調するほか、本ガイドラインは、違法コンテンツの検知・識別・無効化措置（具体例を含む）に対する GDPR 第 6 条(1)(c)または(f)の法的根拠が成立する条件を明確化する。

DSA が要求する通知・対応メカニズム及び内部苦情処理システムも、特にサービスプロバイダが違法コンテンツ報告メカニズムを導入する必要があることから、パーソナルデータの処理を必要とする可能性がある。ホスティングプロバイダは必要な個人データのみを収集すべきであり、通知メカニズムは、情報が違法コンテンツに該当するか否かの判断に通知者の身元確認が必須でない限り、通知者の身元確認を可能とするが必須とすべきではない。通知者の身元を影響を受けるサービスの取得者に開示する必要がある場合、通知者は適切に通知されるべきである。DSA 第 20 条に基づく苦情処理メカニズム及び DSA 第 23 条に基づくアカウント停止は、データ管理者として機能するオンラインプラットフォームプロバイダに対して、データ対象者が GDPR に基づき利用可能な権利及び救済措置を損なうものではない。

DSA 第 25 条(2)は、オンラインプラットフォームプロバイダがインターフェースに欺瞞的な設計パターンを展開することを禁じる同条(1)の規定は、GDPR の適用対象となる当該プロバイダの慣行には適用されない旨を定める。ガイドラインでは、欺瞞的な設計パターンが GDPR の適用対象となるかを評価する際に考慮すべき主要要素、特に個人データの処理が行われているか、および当該パターンが影響を与えるデータ対象者の行動がパーソナルデータの処理に関連しているかについて言及している。これらの主要要素は、欺瞞的な設計パターンが GDPR の適用対象となる場合とならない場合の事例によって補完されている。

DSA 第 26 条は、オンラインプラットフォームプロバイダに対し、インターフェース上で提示する広告についてサービス取得者への透明性を義務付け、プロファイリングに基づく広告提示のための特別カテゴリーデータの使用を禁止している。DSA 第 26 条に基づく情報提供はパーソナルデータの処理発生後に行われるのに対し、GDPR 第 13 条に基づく透明性要件では個人データ取得時に情報を提供することが求められる。DSA 第 26 条(3)に基づく特別カテゴリーのデータ使用禁止は、GDPR 第 9 条(1)および第 22 条(4)の禁止事項を補完するものであり、オンラインプラットフォームプロバイダが GDPR 第 6 条(1)に基づく適切な法的根拠および GDPR 第 9 条(2)に基づく適切な例外規定に依拠して処理を行う場合であっても適用される。

オンラインプラットフォームプロバイダは、ユーザーに表示されるコンテンツの順序や目立ち度をパーソナライズするため、レコメンデーションシステムにおいてユーザーの個人データを利用することがあります。レコメンデーションシステムは、個人データの推論・統合の正確性・透明性、および大規模／機微な個人データ処理に伴う潜在リスクについて懸念を生じさせる。欧州データ保護委員会（EDPB）は、特に個人に重大な影響を及ぼし得る場合、レコメンデーションシステムを介したオンラインプラットフォーム利用者への特定コンテンツ提示がGDPR 第 22 条(1)の意味における「決定」に該当する可能性を排除できないと指摘する。オンラインプラットフォームプロバイダは、ユーザーにレコメンダーシステムの異なる選択肢を提供する際に、それらを平等に提示すべきであり、プロファイリングに基づくレコメンダーシステムの選択肢をユーザーに選択させるよう誘導してはならない。プロファイリングに基づかない選択肢が有効な間は、オンラインプラットフォームプロバイダはユーザーのプロファイリングを目的とした個人データの収集・処理を継続してはならない。

EDPB は、オンラインプラットフォームを利用する未成年者に対する高い水準のプライバシー、安全、セキュリティを確保するという DSA の目的を歓迎する。本ガイドラインは、DSA 第 28 条(1)項及び(2)項が、当該処理が必要かつ比例的である場合に限り、GDPR 第 6 条(1)(c)に基づく個人データの処理の法的根拠となり得ると認める。この必要性と比例性は、データ管理者側が立証すべきものである。オンラインプラットフォームにおける未成年者の安全・セキュリティは、プラットフォーム全ユーザーのプライバシー尊重及び個人データ保護の必要性と均衡を図るべき重大かつ増大する懸念事項である。したがって EDPB は、オンラインプラットフォームプロバイダが特に、ユーザーの明確なオンライン識別を可能とする年齢確認メカニズムを回避すべきであり、年齢推定プロセスに基づくサービス取得者の年齢・年齢層の推定・検証及び恒久的保存を行ってはならないと考える。

DSA 第 34 条及び第 35 条は、超大規模オンラインプラットフォーム及びオンライン検索エンジンのプロバイダに対し、違法コンテンツの拡散（ ）やプライバシー・個人データ保護といった基本的権利へのリスクを含む、サービスに伴うシステミックリスクの管理を義務付けている。GDPR に基づくデータ最小化及び設計時・デフォルト時におけるデータ保護要件の適切な実施は、これらのサービスで識別されたシステム的リスクへの対応に寄与し得る。システム的リスクが識別された場合、GDPR 下ではデータ保護影響評価の実施が義務付けられる可能性が高い。

EDPB は、DSA に基づいて策定される行動規範と GDPR との関係性を明確にし、後者を策定する際には、必要に応じてデータ保護当局の関与を確保することが重要であると考えている。

デジタルサービスコーディネーター、欧州委員会、およびデータ保護当局（後者が加盟国レベルで DSA の管轄当局として指定されていない場合でも）間の協力は、DSA および GDPR の一貫した適用を確保するために極めて重要である。誠実な協力の原則は、こうした当局が協力することを要求しており、つまり、仲介サービスプロバイダ、管理者、または処理者の行為が、相手方の監督下にある枠組みの規定と整合しているかどうかを審査するよう求められた場合、相互に協議すべきであることを意味する。相互協議は、法的確実性を高め、両方の枠組みの適用における規制の不整合や二重裁判のリスクを回避するために重要である。

目次

エグゼクティブサマリー 2

1 序論及び本ガイドラインの適用範囲 6

1.1 DSA と GDPR の関係 8

2 特定の問題点 10

2.1 違法なコンテンツに関する自主的な調査と法令遵守（第 7 条） 10

2.2 通知・措置メカニズムおよび内部 苦情処理システムにおけるパーソナルデータの処理（第 16 条、第 17 条、第 20 条および第 23 条） 15

2.2.1 通知・措置メカニズムに関連する処理活動（DSA 第 16 条及び第 17 条） 15

2.3 欺瞞的な設計パターン（第 25 条） 19

2.4 広告の透明性と、特別なカテゴリーのデータを用いたプロファイリングに基づく広告表示の禁止（第 26 条） 21

2.4.1 広告に関する一般的な透明性義務 21
2.4.2 自動化された個別意思決定およびプロファイリングに関する法的枠組み（ ） 22
2.4.4 広告透明性義務から生じるデータの安全性及び機密性 25

2.5 レコメンダーシステム（第 27 条及び第 38 条） 26

2.6 未成年の防御（第 28 条） 29

2.7 リスクアセスメントと緩和（第 34 条及び第 35 条） 32

2.8 行動規範（オンライン広告を含む）（第 45 条、第 46 条及び第 47 条）並びに GDPR 第 40 条に基づく行動規範との関係 35

2.9 ガバナンスと執行（ ） 36

2.9.1 管轄当局間の協力および DPA との誠実な協力の義務 36

欧州データ保護会議

2016 年 4 月 27 日に欧州議会および理事会が、パーソナルデータの処理およびそのようなデータの自由な移動に関する自然人の保護、ならびに指令 95/46/EC の廃止について定めた規則 2016/679/EU（以下「GDPR」）の第 70 条(1)(e)を考慮し、

EEA 協定、特に 2018 年 7 月 6 日付 EEA 合同委員会決定第 154/2018 号（[1] ）により改正された同協定附属書 XI 及び議定書 37 を考慮し、

その手続規則第 12 条及び第 22 条を考慮し、

DSA と GDPR の相互作用に関する以下のガイドラインを採択した。

[1]本文書における「加盟国」の言及は、「EEA 加盟国」を指すものと理解されるべきである。

1 序論及び本ガイドラインの適用範囲

1. 規則（EU）2022/2065[2]（以下「デジタルサービス法」または「DSA」）は、安全で予測可能かつ信頼できるオンライン環境を確保し、オンライン上での違法コンテンツの拡散や、偽情報その他のコンテンツの拡散が生じうる社会的リスクに対処することを目的として、域内市場における仲介サービスに適用される規則を完全に調和させるものであり、EU 基本権憲章（以下「憲章」）に定められた基本的権利が効果的に保護される枠組みを定める。[3]DSA は 2022 年 10 月 19 日に採択され、2024 年 2 月 17 日に全面施行されたが、一部の規定は 2022 年 11 月 16 日に既に適用開始されている。[4]DSA の対象となる様々な仲介サービスプロバイダのうち、超大規模オンラインプラットフォーム（VLOP）および超大規模オンライン検索エンジン（VLOSE）のプロバイダは、欧州委員会による指定日から 4 ヶ月以内に特定の義務を遵守しなければならない。欧州委員会が現在指定している VLOP および VLOSE は、欧州委員会のウェブサイトで確認できる。[5]

2. 仲介サービスプロバイダは、個人データを処理する場合、GDPR 下では通常、処理の目的と手段を決定するか（これにより管理者として該当）、管理者の指示に基づき管理者のためにデータを処理するだけか（これにより処理者として該当）によって、管理者または処理者として分類されます。[6] 結果として、DSA と GDPR の両方が同一事業体のパーソナルデータの処理を対象とする可能性があります。DSA は、DSA の対象となる各種仲介サービスプロバイダ（特に単なる伝送、キャッシュ、ホスティングサービスプロバイダ）に対し、個人データ処理活動のレベルに応じて異なる義務を課します。この点において、DSA はホスティングサービスプロバイダのサブカテゴリー、特にオンラインプラットフォームプロバイダに対して、著しく多くの義務を課している。[7]さらに、オンラインプラットフォームおよびオンライン検索エンジンは、EU 域内で月間平均アクティブ取得者数が 4,500 万以上に達する場合、欧州委員会によりそれぞれ VLOP（超大規模オンラインプラットフォーム事業者）または VLOSE（超大規模オンライン検索エンジン事業者）に指定される可能性がある。[8] この地位により、

---

[2]欧州議会及び理事会によるデジタルサービス単一市場に関する規則（EU）2022/2065（デジタルサービス法）及び指令 2000/31/EC の改正、OJ L 277、2022 年 10 月 27 日、p. 1。

[3]DSA 第 9 項（前文）。

[4]4 DSA 第 93 条。

[5]欧州委員会、DSA に基づく指定超大規模オンラインプラットフォーム及び検索エンジンの監督、https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses。

[6]GDPR 第 4 条(7)項及び(8)項、並びに GDPR における管理者及び処理者の概念に関する EDPB ガイドライン 07/2020（バージョン 2.1、2021 年 7 月 7 日採択）を参照。

[7]DSA 第 3 条(i)項によれば、「オンラインプラットフォーム」とは「サービスの取得者の要請に基づき、情報を保存し公衆に伝達するホスティングサービスを指す。ただし、当該活動が他のサービスの付随的かつ純粋に補助的な機能である場合、または主たるサービスの付随的機能であり、客観的・技術的理由により当該他のサービスなしでは利用不可能であり、かつ当該機能の他のサービスへの統合が本法の適用回避を目的とするものではない場合を除く」と定義される。前文 14 は「欧州議会及び理事会指令*(EU)2018/1972* で定義される電子メールやプライベートメッセージングサービスなどの対人コミュニケーションサービスは、通信発信者によって決定される有限数の者間の対人コミュニケーションに使用されるため、オンラインプラットフォームの定義の範囲外である」と明確化している。ただし、本規則でオンラインプラットフォームプロバイダに定められた義務は、コミュニケーションの送信者によって決定されない潜在的に無制限の取得者（例：公開グループやオープンチャネルを通じたもの）に対して情報の提供を可能にするサービスには適用される可能性がある。情報の提供が、当該情報を提供したサービスの取得者による直接的な要求に基づいて行われる場合に限り、本規則の意味における公衆への情報提供とみなされるべきである。」[(8)]

[8]DSA 第 33 条(1)項及び(4)項。

DSA 第 III 章第 5 節[9] に列挙される追加義務（パーソナルデータの追加処理を要求するもの）の遵守が求められる。

3. DSA の複数の規定は、GDPR に基づく「プロファイリング」や「特別な種類のデータ」といった定義・概念を含む個人データ保護を特に言及しているが、これは DSA の監督下にある管轄当局による、DSA の特定の規制目的の実施という文脈と目的において行われるものである。

4. 両規制の対象となるプロバイダによる DSA と GDPR の一貫した解釈・適用を確保することは重要である。特に、DSA の規定が仲介サービスプロバイダによるパーソナルデータの処理に影響を与え、GDPR の定義や概念を具体的に参照する場合に当てはまる。例えば、DSA 第 28 条(2)及び第 26 条(3)は、オンラインプラットフォームによる特定種類の広告に関する禁止事項を課す際、GDPR 第 4 条(4)に基づくプロファイリングの定義を参照している。第 26 条(3)に規定される禁止事項は、GDPR 第 9 条(1)に基づく個人データの特別なカテゴリーのリストにも依拠している。このような規定、および仲介サービスプロバイダによる個人データの処理を必要とするその他の規定は、適用される場合には、GDPR および e プライバシー指令の規定と整合的に解釈されるべきである。[10]

5. 本ガイドラインの目的は、DSA の対象となる状況において個人データを処理する際に、仲介サービスプロバイダが GDPR をどのように解釈し適用すべきかを明確にすることである。本ガイドラインの目的は、DSA そのものを解釈することではない。DSA に基づく管轄当局（VLOP および VLOSE に関しては欧州委員会を含む[11]）―欧州デジタルサービス委員会（EBDS）[12] の支援のもと―および EU 裁判所がこれを行うものである。本ガイドラインは、DSA の規定の一部が仲介プロバイダによるパーソナルデータの処理に関わり、GDPR の概念や定義を参照している点において、DSA 及び GDPR の一貫した解釈と適用に寄与することを目的としている。

6. 政治広告に関する追加のデータ保護義務は、政治広告の透明性とターゲティングに関する規則（EU）2024/900 から生じる。さらに、欧州委員会は DSA 第 40 条(13)に基づく委任規則を公表し、超大規模オンラインプラットフォームまたは超大規模オンライン検索エンジンのプロバイダが、DSA 第 40 条に基づき研究者とデータ（個人データを含む）を共有する技術的条件を定めている。[13]上記の事項は本ガイドラインの対象外であり、EDPB はこれらの文脈における GDPR の一貫した適用を確保するため別途取り組む。

---

[9]DSA 第 III 章第 5 節は、超大規模オンラインプラットフォーム及び超大規模オンライン検索エンジンのプロバイダに対し、システミックリスクを管理するための追加的義務を定めている。

[10]DSA 第 2 条(4)(g)。

[11]DSA 第 56 条(2)及び(3)。

[12]DSA 第 61 条(2)は「理事会は、本規則に従い、以下の目的を達成するため、デジタルサービス調整官及び委員会に助言を行うものとする：*(a)* 本規則の対象事項に関する本規則の一貫した適用及びデジタルサービス調整官と委員会の効果的な協力への貢献；*(b)* 本規則の対象事項に関して、域内市場全体で生じている新たな課題について、委員会及びデジタルサービス調整官並びにその他の管轄当局によるガイドライン及び分析の調整及び貢献を行うこと。」DSA 第 63 条(1)も参照のこと。

[13]欧州議会及び理事会規則（EU）2022/2065 を補足する 2025 年 7 月 1 日付欧州委員会委任規則（超大規模オンラインプラットフォーム及び超大規模オンライン検索エンジンのプロバイダが審査済み研究者とデータを共有するための技術的条件及び手続を定めるもの）、C(2025) 4340 final。

1.1 DSA と GDPR の関係

7. EDPB は、DSA と GDPR が異なるが補完的な目的を追求していることを認識している。GDPR がパーソナルデータの処理に関して個人を防御することを目的とする一方、DSA は「安全で予測可能かつ信頼できるオンライン環境を確立するための調和された規則を定めることにより、仲介サービスに関する域内市場の適切な機能に貢献し、イノベーションを促進するとともに、憲章に定められた基本的権利（消費者保護の原則を含む）が効果的に防御される環境を実現すること」を目的としている[14] 。

8. DSA 第 2 条(4)(g)は、DSA が、域内市場における仲介サービスの提供の他の側面を規制する、または DSA を特定・補完する他の連合法的行為（特に GDPR 及び e プライバシー指令）によって定められた規則を損なうものではないと規定している。DSA の序文 10 項は、個人データの処理に関する個人の保護は、この主題に関する連合法の規則、特に GDPR および e プライバシー指令によって規律されることを明記している。

9. したがって、DSA は特別法として、GDPR に基づくパーソナルデータの処理に関する一般規則や、e プライバシー指令に基づく電子通信分野におけるパーソナルデータの処理に関して GDPR を具体化する規則から例外を認めないことは明らかである。[15]しかしながら、欧州連合司法裁判所（CJEU）の確立した判例法によれば、同等の法的地位を有する二つの EU 法令（DSA と GDPR など）が互いに優先順位を定めていない場合、それらを互いに整合的な方法で適用し、一貫した運用を可能とすべきである。[16]

10. DSA に基づく仲介サービスプロバイダにも該当する管理者及びデータ処理者による GDPR の適用を監視する際、データ保護監督当局は、GDPR と DSA の両方に該当する処理活動に関して EU 法の互換的かつ一貫した適用を確保するため、DSA の関連規定（特に各種仲介サービスプロバイダの義務に関する規定）を考慮する必要がある。これは特に、DSA が仲介サービスプロバイダによるパーソナルデータの処理に関して（少なくとも間接的に）GDPR 自体よりも制限的な規則を課す場合に当てはまる。

11. この整合的な適用を確保する取り組みにおいて、EDPB は、基本権としての個人データ保護が、基本権憲章および EU 機能条約（TFEU）の文脈において有する特筆すべき重要性を強調する。[17]したがって、EDPB は、DSA と GDPR の一貫した解釈が、EU の一次法および二次法に定められたプライバシーとデータ保護に関する基本的権利の保護水準を低下させるべきではないことを強調することが重要であると考えてい

---

[14] DSA 第 1 条(1)。

[15] e プライバシー指令と GDPR の相互関係、特にデータ保護当局の権限・任務・権能に関する EDPB 意見書 5/2019、2019 年 3 月 12 日採択、38 項。

[16] 2018 年 5 月 3 日付一般裁判所判決（マルタ対欧州委員会、T-653/16、ECLI:EU:T:2018:241、137 項）：「規則第 *1049/2001* 号及び第 *1224/2009* 号のいずれの規定も、一方の規則を他方より優先させる旨を明示的に定めていない。したがって、これらの規則が互いに整合的な方法で適用され、かつそれらの一貫した適用を可能とするよう確保することが適切である（類推により参照：*2010* 年 *6* 月 *29* 日判決、欧州委員会対 *Bavarian Lager* 事件、*C-28/08 P*、*EU:C:2010:378*、*56* 項、及び *2012* 年 *6* 月 *28* 日判決、欧州委員会対エディション・オディール・ジャコブ事件、*C-404/10 P*、*EU:C:2012:393*、*110* 項を参照）。」判決 139 項及び 140 項はさらに、たとえ「規則第 *1224/2009* 号第 *113* 条*(2)*及び*(3)*が、それ自体として文書への公衆のアクセスに関する一般規則を定めた規則第 *1049/2001* 号から例外を認める特別法（lex specialis）ではないとしても、…前述の *137* 項で述べられたように、規則第 *1049/2001* 号と規則第 *1224/2009* 号の両方が一貫して適用されるべきであるという事実は変わらない。」

[17] シュプナー司法官補佐官による意見書（2023 年 5 月 11 日付、事件番号 C-33/22 オーストリアデータ保護庁、ECLI:EU:C:2023:397、61～78 項）。特に、第 64 項は「当該規定に定められた自然人の個人データ保護を受ける権利は、条約に附属する憲章に含まれる他の基本的権利と比較して、特に重要な意義を有する」と述べている。(18)

る。以下のセクションでは、仲介サービスプロバイダによる個人データの処理に影響を与える DSA の主要規定と GDPR との間で、一貫した適用を確保する方法に関するガイダンスを提供することを目的としている。

2 特定の問題点

2.1 違法なコンテンツに関する自主的な調査と法令遵守（第 7 条）

12. DSA 第 4 条から第 6 条は、特定の条件下で情報の伝送および／または保存を可能にする単なる伝送路、キャッシュ、ホスティングサービスプロバイダに対する責任免除を定めている。例えば、違法コンテンツについて実際の認識がなく、かつ損害賠償請求に関して違法性が明らかな事実や状況を認識していないホスティングサービスプロバイダは、当該違法コンテンツの保存（プロバイダがオンラインプラットフォームである場合は拡散を含む）に起因してサービスの取得者またはサードパーティが被った損害について責任を負わない。[18]

13. 責任免除規則が、仲介サービスプロバイダが自発的に違法コンテンツの検知・対処に向けた措置を講じるインセンティブを損なわないよう、DSA 第 7 条は「仲介サービスプロバイダは、第 *4* 条、*5* 及び *6* 条に定める免責の対象外とはみなされない」と規定している。ただし、DSA 第 8 条は、DSA が仲介サービスプロバイダに対し、伝送または保存する情報の監視、あるいは違法行為を示す事実や状況の積極的探索に関する一般的な義務を課すものではなく、EU 法および加盟国法もこれを課すことはできないことを明確にしている。[19]

14. 違法コンテンツの検知、識別、対処（例：収益化停止、削除、アクセス無効化）または EU 法遵守を確保するための必要な措置を講じるための自動化または非自動化の自主的取り組みは、仲介サービスプロバイダによる個人データの処理を伴う可能性がある。[20]こうした取り組みでは、機械学習（ML）技術に基づくモデル（ ）の展開など、パーソナルデータの処理を伴う複数の異なる技術に依存する場合がある。これらのモデルは、機械の事前学習に基づいて特定のコンテンツ項目の特性を認識できる。多くの場合、コンテンツが違法コンテンツに該当するか否かを予測するために大量のデータを必要とし、形状、質感、色、テキストの分析に使用される。平文環境では、マルチメディアベースまたはテキストベースの機械学習ツールが違法コンテンツの検知に活用される（例：キーワードやテキストパターンマッチングによる）。このようなモデルの訓練および違法コンテンツの検知・識別・対処の一環としての展開において、プロバイダはパーソナルデータの処理に関する原則（最小化原則など）および GDPR に由来する設計時およびデフォルト時のデータ保護義務への準拠を慎重に検討し、実証する必要があります。[21] 可能な限り、これらの措置はパーソナルデータの処理を伴わないべきである。

15. 違法コンテンツの自主的検知・対処技術は、自動化された手法によるデータ対象者の活動に対する体系的な監視を伴う可能性があり、これによりデータ対象者の不正行為への関与について誤った結果や不正確な

[18]DSA 第 6 条(1)(a)。

[19]同様の規則は、欧州議会及び理事会による 2000 年 6 月 8 日付指令 2000/31/EC（情報社会サービス、特に電子商取引に関する特定の法的側面、特に電子商取引に関する指令）第 15 条からも既に導かれていた（OJ L 178, 2000 年 7 月 17 日, p. 1–16）。参照：欧州司法裁判所判決（2022 年 4 月 26 日、ポーランド対欧州議会及び理事会、C-401/19）、ECLI:EU:C:2022:297、90 項、ならびに欧州司法裁判所 2019 年 10 月 3 日付判決、Eva Glawischnig-Piesczek 対 Facebook Ireland Limited、C-18/18、ECLI:EU:C:2019:821、41-46 項を参照。

[20]こうした活動は、デジタルサービス法（DSA）第 3 条(t)項における「コンテンツモデレーション」の定義に近いものの、より狭い範囲に属する。同項では「仲介サービスプロバイダが、特に、サービスの取得者によって提供された違法なコンテンツまたは利用規約に反する情報を検知、識別、対処することを目的として行う活動（自動化されているか否かを問わない）であり、当該違法コンテンツまたは情報の利用可能性、可視性、アクセス可能性、可視性、利用可能性に影響を与える措置（降格、収益化停止、アクセス無効化、削除など）や、サービス取得者が当該情報を提供する能力に影響を与える措置（取得者のアカウント停止・一時停止など）を含む」

[21]GDPR 第 5 条及び第 25 条。

結果が生じる恐れがある。これは結果としてデータ対象者に重大な悪影響（例：アカウント停止による評判毀損、合法コンテンツに関する表現の自由の制限など）をもたらしうる。データ保護の観点では、これらの技術の使用は公平性とデータ正確性のリスクを伴う。これらのリスクは、既存技術（パターン認識など）の誤認識率が比較的高い傾向にある事実によってさらに増幅される。[22] さらに、特に VLOP（大規模オンラインプラットフォーム事業者）や VLOSE（大規模オンラインサービス事業者）といった仲介サービスにおいては、ユーザー数と共有コンテンツ数が膨大なため、違法コンテンツの自主的検知・対処技術の誤認識率が比較的低くとも、絶対的な誤認識件数が多大になる可能性がある。

16. 違法コンテンツの識別のためにパーソナルデータの処理が必要な場合、DSA は、DSA 第 7 条に該当するそのような処理がどの程度正当かつ比例的であるかを明示していない。したがって、また DSA における「違法コンテンツ」の広範な定義を考慮すると、[23] 仲介プロバイダが GDPR に準拠しつつ DSA 第 7 条に基づく自主的な自主的措置をどのように実施できるかを概説することが重要である。[24]

17. DSA 第 7 条が対象とする最初のシナリオは、仲介サービスプロバイダが**違法コンテンツの**検知・識別・削除（またはアクセス無効化）のための自主的調査その他の措置の文脈で処理を行う場合である。GDPR に準拠するためには、この処理はデータ対象者に対して合法的・公正かつ透明性をもって行われ、[25] GDPR 第 5 条の残りの原則および GDPR がデータ管理者（controller）に課す義務を遵守しなければならない。まず第一に、仲介サービスプロバイダ（管理者として）は、このような処理を実施するための GDPR 第 6 条(1)に基づく法的根拠を識別する必要があります。管理者はこれらの目的のために処理を実施する法的義務を負わないため、このシナリオで利用可能な最も適切な法的根拠は GDPR 第 6 条(1)(f)（「正当な利益」）となる。

18. 正当な利益の法的根拠に依拠するには、管理者は以下の 3 つの累積的条件を満たす必要がある：[26] 追求される利益が正当であること；パーソナルデータの処理が追求される正当な利益の目的のために必要であること；データ処理の対象となるデータ対象者の利益または基本的権利・自由が、管理者が追求する正当

---

[22]欧州議会調査局、児童の性的虐待の防止及び対策に関する規則案－補足影響評価、PE 740.248、2023 年 4 月、82 頁。関連資料：欧州データ保護委員会（EDPB）と欧州データ保護監督官（EDPS）による共同意見書 04/2022「児童の性的虐待を防止しこれと闘うための規則を定める欧州議会及び理事会規則案に関する意見」、2022 年 7 月 28 日採択、パラグラフ 40、61；及び児童の性的虐待を防止し対策するための規則を定める規則案に関する立法動向に関する EDPB 声明 1/2024、2024 年 2 月 13 日採択。

[23]デジタルサービス法（DSA）第 3 条(h)：「違法なコンテンツ」とは、その内容自体または活動（製品の販売やサービスの提供を含む）に関連して、*EU* 法または *EU* 法に準拠する加盟国の法律に適合しない情報を指す。当該法律の具体的な主題または性質にかかわらず。DSA 前文第 12 項は、「『違法コンテンツ』の概念は、違法コンテンツ、製品、サービス及び活動に関連する情報を広く包含するよう定義されるべきである。特に、この概念は、適用法の下で、それ自体が違法である情報（違法なヘイトスピーチやテロ関連コンテンツ、違法な差別的コンテンツなど）、あるいは適用される規則により違法活動に関連するという事実から違法とみなされる情報を、その形態を問わず指すものと理解されるべきである。」具体例としては、児童性的虐待を描写する画像の共有、私的画像の違法な非合意共有、オンラインストーキング、非適合製品または偽造製品の販売、消費者保護法に違反する製品販売またはサービス提供、著作権保護対象物の無断使用、違法な宿泊サービスの提供、生きた動物の違法販売などが挙げられる。」

[24]また、GDPR が適用される範囲において、例えば、サービスの取得者の純粋に個人的または家庭内活動以外の活動（GDPR 第 2 条(2)(c)参照）が該当します。

[25]GDPR 第 5 条(1)(a)。

[26]欧州司法裁判所判決（2019 年 12 月 11 日 Asociaţia de Proprietari bloc M5A-ScaraA, C-708/1, ECLI:EU:C:2019:1064）40 項；GDPR 第 6 条(1)(f)に基づくパーソナルデータの処理に関する EDPB ガイドライン 1/2024、バージョン 1.0、2024 年 10 月 8 日採択、第 II 章。

な利益を上回らないこと。特にオンラインプラットフォームを通じて公衆に拡散される可能性のある違法コンテンツを、サービス取得者を防御する目的で仲介サービスにおいて検知・対処する利益は、明らかに正当である。[27]他の二つの条件に関しては、管理者は、追求される正当な利益が、データ保護という基本的権利に対する制約がより少ない他の手段によって同様に効果的に達成されることが合理的に期待できないことを実証する必要がある。[28] さらに、データ対象者の利益、権利、自由と管理者が追求する利益との間の均衡テストを実施する際、管理者は、処理がデータ対象者によって合理的に予想されるかどうか、[29] およびそれが子どもに関係するかどうかについて特に注意を払うべきである。[30]仲介サービスプロバイダ（管理者として）は、処理によって追求される具体的な正当な利益について、[31] データ対象者に通知するために必要なあらゆる措置を講じるべきであり、また、データ最小化の原則に沿って、違法なコンテンツの検知、識別、除去（またはアクセスを無効化）するために管理者が想定する具体的な措置について通知すべきである。

19. 第 7 条 DSA が対象とする第二のシナリオは、仲介プロバイダが、**EU 法および EU 法に準拠した国内法の要件を遵守するため**、誠実かつ注意深く処理を行う場合である。実際、DSA 第 8 条は EU または加盟国が仲介サービスプロバイダに対し、伝送または保存する情報の監視や違法行為を示す事実・状況の調査といった一般的な義務を課すことを禁じているが、EU 法または加盟国法に基づき、違法コンテンツを検知・対処する対象を絞った法的義務が課される可能性がある。

例 *1* – オンラインコンテンツ共有サービスにおける著作権保護作品の識別と削除

ある企業は、主に、または主な目的の一つとして、ユーザーがアップロードした著作権保護作品その他の保護対象物を大量に保存し、公衆がアクセスできるようにする仲介サービスを提供している。同社は営利目的でこれらのコンテンツを整理・促進しており、したがって指令(EU)2019/790（[32] ）（「著作権指令」）に基づくオンラインコンテンツ共有サービスプロバイダに該当する。本指令の下では、当該企業は、著作権保護対象作品の公衆への伝達（公衆への提供を含む）に関する無断行為について責任を負う。ただし、一定の条件を満たしたことを証明できる場合はこの限りではない。これらの条件の中には、権利者からの通知を受け

[27]仲介サービスプロバイダが違法性の疑いのあるコンテンツを識別した場合の法執行機関との個人データ共有については、欧州司法裁判所 2023 年 7 月 4 日付判決 Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537 を参照のこと。同判決第 124 項では以下のように明確化されている。「付託裁判所が言及した、犯罪の防止、検知及び訴追を目的とした法執行機関との情報共有に関する目的については、原則として、*GDPR* 第 *6* 条*(1)*項第 *1* 文*(f)*号の意味における管理者が追求する正当な利益を構成し得ないものと認められる。*Meta Platforms Ireland* のような民間事業者は、その経済的・商業的活動とは無関係であるこのような正当な利益に依拠することはできない。逆に、当該事業者が遵守すべき法的義務の履行のために客観的に必要である場合には、この目的が当該事業者による処理を正当化し得る GDPR 第 6 条(1)(f)に基づくパーソナルデータの処理に関する EDPB ガイドライン 01/2024（バージョン 1.0）第 131 項・第 132 項も参照のこと。同項は、GDPR の前文 50 を考慮した上で、管理者が GDPR 第 6 条(1)(f)に依拠して法執行機関と情報を共有できる状況について述べている。

[28]これには、GDPR 第 5 条(1)(c)に基づくデータ最小化の原則の遵守も含まれる。2023 年 7 月 4 日付欧州司法裁判所判決 Meta Platforms 他、C-252/21 ECLI:EU:C:2023:537、パラグラフ 108 および 109 参照。

[29]2023 年 7 月 4 日付欧州司法裁判所判決 Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537、パラグラフ 112。

[30]GDPR 前文 38 項。参照：欧州司法裁判所判決（2023 年 7 月 4 日）Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537、111 項及び 123 項。

[31]GDPR 第 13 条(1)(c)及び(d)。2023 年 7 月 4 日付欧州司法裁判所判決 Meta Platforms 他事件（C-252/21、ECLI:EU:C:2023:537）第 126 項も参照。

[32]欧州議会及び理事会指令（EU）2019/790（2019 年 4 月 17 日）デジタル単一市場における著作権及び関連権利に関する指令、並びに指令 96/9/EC 及び 2001/29/EC の改正、OJ L 130、2019 年 5 月 17 日、92–125 頁

た場合、業界の高い専門的注意義務基準に従い、特定作品の 利用不可化及び再アップロード防止を最大限努力して確保することが企業に求められる。[33]このような最善の努力を実施するために企業が個人データを処理する必要が生じる場合があるが、当該処理は、指令 2002/58/EC および規則(EU)2016/679 に従う場合を除き、個々のユーザーの特定につながるものであってはならず、またパーソナルデータの処理であってはならない。[34]

20. EU 法に基づく要件により仲介サービスプロバイダが個人データの処理を義務付けられる別の事例としては、データ対象者が自身の個人データが違法に処理された（例：データ主体の同意またはその他の法的根拠なしに、サービスの取得者がオンラインプラットフォームを通じて拡散した場合）として、GDPR 第 17 条に基づく消去権を行使する場合が挙げられる。GDPR 第 17 条に基づく義務を遵守するため、仲介サービスプロバイダは、違法と主張されるコンテンツを検知し、GDPR 第 17 条(3)に基づく例外が適用されるかどうかを慎重に検討した上で、個人データを消去すべきかどうかを決定する必要があるかもしれない。

21. パーソナルデータの処理を必要とする範囲において、法的義務は GDPR 第 6 条(1)(c)に基づく処理の法的根拠となり得る。説明責任の原則に沿い、仲介サービスプロバイダは既存の法的義務遵守に必要なパーソナルデータの処理の範囲を特定すべきである。いずれの場合も、欧州司法裁判所（CJEU）の判例法に従い、当該法的義務は明確かつ正確であり、その適用対象者にとって予測可能でなければならない。[35] さらに、法律はパーソナルデータの処理を規定する措置がどのような状況・条件下で採用され得るかを明示し、干渉が厳密に必要な範囲に限定されることを保証しなければならない。[36]さらに、GDPR 第 6 条(1)(c)に基づく処理は、追求される正当な目的に比例したものでなければならない。すなわち、目的達成に同等の効果を持ちながら、より侵襲性の低い代替手段が存在してはならない。[37]違法コンテンツへの対応またはサービスの一人または複数の特定の取得者に関する 情報の提供を命じる管轄当局の命令に従う文脈で処理が行われる場合、仲介プロバイダは、当該命令が DSA 第 9 条または第 10 条に定められた要件を満たし、GDPR 第 6 条(1)(c)に基づく処理を正当化できるかどうかも確認する必要がある。EDPB はさらに、DSA の理由 56 が「DSA は、ホスティングサービスプロバイダによる犯罪行為の特定を目的としたサービス取得者のプロファイリングの法的根拠を提供しない」ことを明確化している点にも言及している。

22. 処理における自動化のレベル、およびデータ対象者に及ぼす結果に応じて、DSA 第 7 条に該当する活動は、GDPR 第 22 条(1)で**禁止されている、プロファイリングを含む自動処理のみに基づく決定に**該当する可能性がある。[38] 一方で、仲介サービスプロバイダによる違法と主張されるコンテンツの削除決定は、そのコ

[33]著作権指令第 17 条(4)。同指令の前文 66 項はさらに次のように述べている。「オンラインコンテンツ共有サービスプロバイダが、専門的注意義務の高い業界標準に従い最善の努力を払ったかどうかを評価する際には、当該プロバイダが、業界のベストプラクティス、関連する全ての要素及び動向を踏まえた措置の有効性、並びに比例原則を考慮しつつ、自らのウェブサイト上で無許可の著作物その他の対象物へのアクセスを防止するという結果を達成するために、注意深い事業者が講じるであろうあらゆる措置を講じたかどうかを勘案すべきである」.

[34]著作権指令第 17 条(9)。

[35]GDPR 第 41 項の前文。これは、欧州司法裁判所（CJEU）の解釈に基づく基本権憲章第 7 条及び第 8 条の要件を補完するものであり、いかなる干渉も、明確かつ正確で予見可能な法律によって規定されなければならない。

[36]欧州司法裁判所判決 2022 年 6 月 21 日 人権連盟事件 C-817/19, ECLI:EU:C:2022:491, 117 項。

[37]欧州司法裁判所判決 2023 年 11 月 9 日 Gesamtverband Autoteile-Handel eV 対 Scania CV AB, C319/22, ECLI:EU:C:2023:837, 52～62 項。

[38]2023 年 12 月 7 日付欧州司法裁判所判決 OQ 対 ヘッセン州、C-634/21、ECLI:EU:C:2023:957、パラグラフ 52：「*GDPR 第 22 条(1)*は、データ対象者に対し、プロファイリングを含む自動化された処理のみに基づく決定の対象とならない『権利』を付与している。この規定は原則的な禁止事項を定めており、その侵害は当該個人によって個別に主張される

ンテンツが削除されたサービスの取得者に重大な影響を与える可能性がある。[39]他方、違法コンテンツの検知・削除を目的とした個人データの自動処理システムにおいて、人間の関与の程度を評価することは特に重要である。人間の関与が全くない場合、人間の関与が実質的でない場合（[40]）、あるいはコンテンツ削除の判断において人間がシステムが生成したアルゴリズム的推奨に「強く依存」する場合（[41]）、その決定は依然として GDPR 第 22 条(1)に基づく「自動処理のみに基づく決定」とみなされる。GDPR 第 22 条(1)が適用される場合、仲介サービスプロバイダは、GDPR 第 22 条(2)に基づく禁止の例外が適用されるかどうか、特に処理が GDPR 第 22 条(2)(b)の要件を満たす EU または加盟国の法律によって認可されているかどうかを検証する必要があります。[42]さらに、GDPR 第 22 条(1)が適用される場合、仲介サービスプロバイダは、GDPR 第 22 条(4)の条件が満たされない限り、特別なカテゴリーの個人データの処理を避けるべきである。

23. また、仲介サービスプロバイダは、DSA 第 7 条の範囲内で実施する処理に関して、データ対象者に対して**透明性を確保することが**重要である。これには、GDPR 第 12 条に定められた条件に沿い、GDPR 第 13 条及び第 14 条で要求される情報の全要素をデータ対象者にプロバイダすることが含まれる。[43] 処理が GDPR 第 22 条(1)に基づく自動化された意思決定に該当する場合、データ管理者はデータ対象者に対し、当該活動に従事していることを通知し、意思決定に関わる論理について意味のある情報を提供し、処理の意義及び想定される結果を説明しなければならない。[44]DSA 第 14 条(1)および第 15 条(1)(c)・(e)は、コンテンツモデレーション（アルゴリズムによる意思決定および人的レビューを含む）の目的で使用される方針、手順、措置、ツールに関する仲介プロバイダへの追加的な透明性要件を定めている。これには、コンテンツモデレーション目的で使用される自動化された手段の潜在的な誤り率および適用されるあらゆる保護措置の開示も含まれます。さらに、DSA 第 17 条に基づく透明性要件により、ホスティングサービスプロバイダは、サービス

必要はない」。2018 年 2 月 6 日に最終改訂・採択された、規則 2016/679 の目的のための自動化された個別意思決定およびプロファイリングに関する第 29 条データ保護作業部会ガイドライン（WP251rev.01）も参照のこと。

[39]2018 年 2 月 6 日に最終改訂・採択された、規則 2016/679 を目的とした自動化された個別意思決定およびプロファイリングに関する第 29 条データ保護作業部会ガイドライン（WP251rev.01）21 ページ：「データ処理が個人に重大な影響を与えるためには、その処理の影響が注目に値するほど十分に大きく、あるいは重要でなければならない。言い換えれば、当該決定は以下をもたらす可能性を有していなければならない：

- ・関係者の状況、行動、選択に重大な影響を与えること；
- データ対象者に長期的または恒久的な影響を与える；または
- 最も極端な場合、個人の排除または差別につながる」

[40]2016/679 規則に基づく自動化された個別意思決定及びプロファイリングに関する第 29 条データ保護作業部会ガイドライン（WP251rev.01）、最終改訂・採択日：2018 年 2 月 6 日、21 ページ：「データ管理者は、人為的関与を偽装することで第 *22* 条の規定を回避することはできない。例えば、結果に実質的な影響を与えないまま、自動的に生成されたプロファイルを個人に定期的に適用する場合、これは依然として自動処理のみに基づく決定である。人間の関与と認められるためには、管理者は決定に対する監視が単なる形だけの行為ではなく、実質的なものであることを保証しなければならない。それは決定を変更する認可と能力を持つ者によって行われるべきである

[41]欧州司法裁判所判決 2023 年 12 月 7 日 OQ 対 ヘッセン州、C-634/21、ECLI:EU:C:2023:957、62 項および 73 項。

[42]2016/679 規則に基づく自動化された個別意思決定及びプロファイリングに関する第 29 条データ保護作業部会ガイドライン（WP251rev.01）、最終改訂・採択日 2018 年 2 月 6 日、23～24 頁。

[43]より詳細なガイダンスについては、2016/679 規則に基づく透明性に関する第 29 条作業部会ガイドライン（WP260 rev.01）（最終改訂・採択日：2018 年 4 月 11 日）を参照のこと。

[44]2016/679 規則の目的のための自動化された個別意思決定およびプロファイリングに関する第 29 条データ保護作業部会ガイドライン（WP251rev.01）、最終改訂・採択日：2018 年 2 月 6 日、2426 ページ。

取得者が提供した情報が違法コンテンツである、またはサービスの利用規約に違反していることを理由として、DSA 第 17 条(1)に基づく制限を課した場合、影響を受けるサービス取得者に対し、明確かつ具体的な理由の明示を求められる可能性がある。[45]特に、DSA 第 17 条(3)(b)によれば、理由説明には、当該決定が自主的な調査に基づいて行われたか否かに関する情報を含めなければならない。

24. 最後に、**データ保護影響評価**（DPIA）および処理が「高いリスクをもたらす可能性」の判断に関する欧州データ保護委員会（EDPB）ガイドラインによれば、DSA 第 7 条に基づく仲介プロバイダによる自発的または義務的措置は、DPIA の実施が必要であることを示す複数の規準を満たす可能性が高い。こうした規準には、評価またはスコアリング、法的または同等の重大な影響を伴う自動化された意思決定、および体系的な監視が含まれる。VLOP（大規模オンラインプラットフォーム）のプロバイダは、大規模処理の基準も満たす可能性が高い。[46] GDPR 第 36 条に基づき、仲介サービスプロバイダは、GDPR 第 35 条に基づくデータ保護影響評価において、リスク緩和措置を講じない場合、処理が高リスクをもたらすと示された場合には、処理前に監督当局と協議する必要が生じる可能性がある。

2.2 通知・措置メカニズムおよび内部 苦情処理システムにおけるパーソナルデータの処理（第 16 条、第 17 条、第 20 条および第 23 条）

2.2.1 通知・措置メカニズムに関連する処理活動（DSA 第 16 条及び第 17 条）

25. オンライン上の違法コンテンツに対処するため、DSA は、ホスティングサービスプロバイダに対し、個人または事業体が通知を通じて違法コンテンツを報告するのを支援する仕組みを導入する義務を定めている。この目的のため、DSA 第 16 条は、規模の大小を問わず[47] 、オンラインプラットフォームを含むあらゆるホスティングサービスプロバイダが、「通知と対応」メカニズムを導入する義務を負うことを規定している。これにより、個人または事業体が、違法コンテンツとみなす特定の情報項目の存在を電子的手段で通知できるようになる。当該通知を受領したホスティングサービスプロバイダは、そのアセスメントに同意するか否かを判断し、措置（例：コンテンツ削除、表示順位低下、支払い停止・終了その他の金銭的支払い制限などによる可視性制限）を講じるか否かを決定できる。[48]

26. DSA 第 22 条によれば、これらの仕組みは信頼できるフラッガー（すなわち「違法コンテンツ対策において特定の専門知識と能力を有し、かつ勤勉・正確・客観的に活動していることを証明した、個人ではなく事業体」）によっても発動され得る。[49]

27. 特に個人によって開始されるこれらの「通知と措置」システムは、通知を提出した個人（「通知者」）および影響を受けるサービスの取得者（これらが個人である場合）のパーソナルデータの処理を伴う可能性がある。また、違法コンテンツを識別するために、通知または識別されたコンテンツにサードパーティの個人データが含ま

[45]参照：第 34 項。

[46]第 29 条データ保護作業部会ガイドライン「データ保護影響評価（DPIA）及び処理が『高いリスクをもたらす可能性が高い』かどうかを判断するための指針」（WP 248）、2017 年 4 月 4 日採択、7-9 ページ。

[47](50) 前文 DSA は、義務の対象となるプロバイダの種類の例示している。また、「ファイル保存・共有サービス、ウェブホスティングサービス、広告サーバー、ペーストビン（一時保存サービス）が、DSA でカバーされるホスティングサービスに該当する場合」についても言及している。

[48]DSA 第 17 条(1)参照。

[49]DSA 前文第 61 項。DSA 第 22 条(3)によれば、信頼できるフラッガーは、少なくとも年 1 回、第 16 条に基づき提出された通知に関する詳細な報告書を公表しなければならない。当該報告書には個人データを含んではならない。

れる場合、サードパーティの個人データの処理を引き起こす可能性がある。 したがって、このような場合、ホスティングサービスプロバイダは管理者として位置づけられ、GDPR に従って個人データを尊重し処理しなければならない。

28. [50]「通報者」の個人データに関しては、十分に正確かつ適切に裏付けられた通報の提出を促進するため、DSA 第 16 条(2)は、違法コンテンツに関連するその他の情報とともに、通報者の氏名および電子メールアドレスを電子的手段で提出することをホスティングプロバイダが「可能にし」「促進する」ことを想定している。この情報は、児童の性的虐待及び性的搾取並びに児童ポルノの防止に関する指令 2011/93/EU（「CSAM 指令」）第 3 条から第 7 条に規定される犯罪行為に該当すると認められる場合には収集すべきではない。

29. したがって、DSA の規定および通知者が提出した通知に記載されている情報に基づき、ホスティングプロバイダは、通知の受領確認、通知された情報に関する決定、および当該決定に対する救済手段に関する情報を、不当な遅滞なく通知者に提供するために、通知者の氏名および電子メールアドレスを処理する権利を有する。[51]同様に、技術的または運用上の理由により特定情報を削除できない場合、プロバイダにその旨を通知するため、入手可能な氏名および電子メールアドレスを使用すべきである。[52] さらに、「厳密に必要な場合に限り」、影響を受けるサービス取得者に提供される理由説明書には、プロバイダの個人データを含めるべきである。[53]

30. したがって、『通知と措置』システムの機能規則を策定・実施する際には、通知者を含む全ての関係者の個人データに関する権利を防御するための強固な保護措置を設ける必要がある。[54]この点に関して、EDPB は、個人データは DSA 関連規定で言及される特定の目的に必要な範囲に限定されるべきであることを想起する。したがって、例えば、プロバイダは一般的に、DSA 第 16 条(2)で言及されるもの以外の通知者の追加個人データを要求すべきではない。これは、追加的な識別 データが必要と認められる場合、DSA がそれらを明示的に言及していること[55] 、また、前文 50 によれば、「通知メカニズムは、当該情報が違法なコンテンツに該当するか否かを判断するために必要な場合を除き、通知者の識別を可能とするべきであるが、それを要求すべきではない」とされていることを踏まえたものである。したがって、プロバイダは通知者の身元確認を可能とすべきであるが、違法コンテンツを他に方法により特定できない場合を除き、通知の提出を身元提供を条件とすべきではない。

31. 同様に、説明責任の原則に基づき、管理者は、DSA 第 17 条(3)(b)に従い、影響を受けるサービスの取得者に対して通知者の身元を開示することが必要かつ均衡のとれた場合を定義すべきである。すでに前文 54 は、「この情報がコンテンツの違法性を識別するために必要である場合」にこれが起こり得ると明確化して

[50]通知者は、ホスティングサービスプロバイダに対し、違法と疑われるコンテンツについて通知する個人または事業体を指す。

[51]DSA 第 16 条(4)及び(5)参照。

[52]DSA 第 51 項 前文

[53]DSA 第 17 条(3)(b)。

[54]この点に関して、DSA の 52 項は「このような通知および対応メカニズムに関する規則は、これにより、統一的、透明性があり、明確な規則に基づき、通知を適時、慎重かつ恣意的でない方法で処理し、関係する全ての当事者（特に、加盟国における設立地や居住地、問題となっている法分野にかかわらず、憲章によって保障される基本権を含む）の権利及び正当な利益を保護するための強固な保護措置を講じるべきである」と勧告している。

[55]例えば、事業者の追跡可能性に関する DSA 第 30 条を参照のこと。同条は、オンラインプラットフォームプロバイダに対し、事業者の氏名、住所、電話番号、電子メールアドレス、ならびに身分証明書の写しまたはその他の電子的識別手段の取得を義務付けている。

おり、例えば知的財産権侵害の事例に言及している。このような場合、通知者の個人データのうち厳密に必要なもののみが影響を受けるサービスの取得者に伝達されることを確保すべきであり、データ対象者（通知者）は、GDPR 第 13 条に従い、このような処理活動が行われる可能性があることを適切に通知される必要がある。

32. DSA 第 16 条(6)は、ホスティングプロバイダが本制度に基づき受領した通知の処理または意思決定プロセスに自動化された手段を利用できることを想定し、その場合には通知を提出した個人または事業体に対し、当該利用に関する情報を提供することを規定している。これは、適用される場合には自動化された意思決定に関する情報を含め、GDPR 第 13 条に基づき提供される情報に加えて行われるべきである。

33. 欧州データ保護委員会（EDPB）は、本規定がデータ対象者である通知者に対する透明性を高めることを歓迎するとともに、当該削除が GDPR 第 22 条の適用範囲に該当し得る場合、本規定が法的効果を生じさせる、または関係者に同様の重大な影響を及ぼす、プロファイリングを含む自動処理のみに基づく決定に対して厳格な条件を課すことを想起する。特に留意すべきは、データ管理者が従うべき EU 法または加盟国法が、データ対象者の権利・自由・正当な利益を保護する適切な措置を定めており、かつ自動処理のみに基づく決定を認める場合（DSA が想定する通知・措置メカニズム、[56] において想定される通知および措置メカニズムの場合のように、データ対象者が従うべき EU または加盟国の法律によって認可され、かつデータ対象者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が定められる場合を除き、そのような自動化された決定は、データ対象者が明示的な同意を与えた場合、または GDPR 第 9 条(2)(a)または(g)に従い、重大な公共の利益のために処理が必要な場合を除き、特別なカテゴリーの個人データに基づいてはならない。[57]

34. DSA 第 17 条は、ホスティングサービスプロバイダに対し、サービス取得者が提供した特定の情報項目について、アクセス削除または無効化の決定を行う場合、当該情報が違法コンテンツである場合、またはサービスの利用規約に適合しない場合のいずれにおいても、影響を受けるサービス取得者に対し、明確かつ具体的な理由の説明を提供することを義務付ける。この義務は、関連する電子連絡先がプロバイダに知られている場合にのみ適用され、DSA 第 9 条に基づき「関連する国内司法または行政当局から、1 つ以上の特定の違法コンテンツに対して措置を講じるよう命じる命令を受領した場合」には適用されない。[58]

35. DSA 第 17 条(3)(c)は、決定に自動化された手段を用いたことを影響を受ける取得者に通知する義務に言及することで、ホスティングサービスプロバイダが受領した通知を処理または決定するために自動化された手段を利用できる可能性を示唆している。

36. この点に関して、EDPB は、EDPS がデジタルサービス法案に関する意見書 1/2021（[59] ）で既に検討したように、GDPR 第 22 条は、法的効果を生じさせる可能性のある決定、または同様に関係者に重大な影響を与える決定につながる、プロファイリングを含む自動処理のみに基づく決定に対して厳格な条件を課していることを想起する。特に、GDPR 第 22 条(2)(b)は、データ対象者の権利・自由及び正当な利益を保護

[56]GDPR 第 22 条(2)(b)。

[57]GDPR 第 22 条(4)。

[58]DSA 第 17 条(5)。

[59]デジタルサービス法（DSA）提案に関する欧州データ保護監督官（EDPS）意見書 1/2021、2021 年 2 月 10 日、第 42 項。

するための適切な措置を定めた連邦法または加盟国法によって認可される場合に限り、決定を自動処理のみに基づいて行うことを想定している[60] 。

37. ホスティングプロバイダの措置が GDPR 第 22 条に基づく自動化された意思決定に該当するか否かにかかわらず、DSA 第 17 条(3)はホスティングプロバイダに対し、データ対象者（影響を受ける取得者が個人の場合）に対して特定の情報を提供する義務を課している。これには、予定される措置、意思決定の根拠となった事実及び状況、決定に自動化された手段が使用されたか否か、またその決定が自動化された手段を用いて検知または識別されたコンテンツに関してなされたものか否か、法的根拠、当該根拠に基づき当該情報が違法コンテンツと見なされる理由、および当該決定に関してサービスの取得者が利用できる救済の可能性についても提供しなければならない。

2.2.2 苦情処理及び不正利用対策のためのオンラインプラットフォームプロバイダによる影響を受ける取得者のパーソナルデータの処理（第 20 条及び第 23 条）

38. 違法コンテンツ対策活動の枠組みにおいて、DSA 第 III 章第 3 節は、オンラインプラットフォームプロバイダにのみ、個人データの処理を伴う可能性のある追加的義務を課している。

39. DSA 第 20 条に基づき、コンテンツの違法性またはオンラインプラットフォームの利用規約への適合性に関する決定の取得者、および通知を提出した個人（または事業体）は、それぞれ、自身に不利益をもたらす決定に異議を申し立てるため、または提出された通知に基づいて行われた不適切な措置に異議を申し立てるために、苦情を申し立てる権利を有する。[61]欧州データ保護委員会（EDPB）は、いずれの場合においても、DSA がオンラインプラットフォームプロバイダに対し、第 20 条に言及される決定が自動化された手段のみに基づくのではなく、適切な資格を有する職員の監督下でなされることを確保するよう求めている点を歓迎する。[62]EDPB は、この場合においてもオンラインプラットフォームプロバイダは関連する個人データのデータ管理者として行動するため、GDPR の関連規定を遵守すべきであることを改めて指摘する。特に、DSA 第 20 条に基づく苦情処理メカニズムは、データ管理者として行動するオンラインプラットフォームプロバイダに対してデータ対象者が GDPR に基づき有する権利及び救済手段を妨げるものではないことに留意すべきである。

40. さらに、「明らかに違法なコンテンツを頻繁にプロバイダしたり、明らかに根拠のない通知や苦情を頻繁に提出したりするオンラインプラットフォームの悪用は、信頼を損ない、関係者の権利及び正当な利益を害する」ことを考慮すると、[63]DSA 第 23 条は、濫用的行為（すなわち、明白に違法なコンテンツを頻繁に提供する取得者[64] 及び明白に根拠のない通知や苦情を頻繁に提出する通知者・苦情申立者[65] ）に従事する者に対し、オンラインプラットフォームが関連する活動を停止することを認めている。

41. オンラインプラットフォームの悪用に対する保護措置を想定しつつ、DSA はこうした保護措置が「適切、均衡的かつ効果的」であるべきこと、また「憲章に定められた適用される基本的権利と自由を含む、関係する全て

[60]また、欧州司法裁判所判決（2023 年 12 月 7 日 OQ 対 ヘッセン州、C-634/21、ECLI:EU:C:2023:957、65-66 項）も参照のこと。

[61]DSA 第 20 条(1)。

[62]デジタルサービス法（DSA）第 20 条(6)。

[63]DSA 第 63 項（前文）。

[64]DSA 第 23 条(1)。

[65]DSA 第 23 条(2)。

の当事者の権利と正当な利益を尊重する必要がある」ことを規定している。[66] この点に関して、欧州データ保護委員会（EDPB）は、DSA が既に識別している保護措置を歓迎する。[67] これらは、 このようなケースにおける自動化された決定の採用を回避することを可能にする。また、オンラインプラットフォームプロバイダに対し、悪用対策の措置を識別し、利用規約にこの点に関する方針を定める際には、GDPR 第 5 条に定められたすべてのデータ保護原則、特に最小化、正確性、透明性、データ保持の原則の尊重を確保する必要性を考慮に入れるべきであることを改めて想起させる。

42. オンラインプラットフォームプロバイダが、不正行為に関与していると見なす者に対する関連活動を停止する決定は、当該者の権利に重大な影響を及ぼす可能性がある。このため、不正確な個人データの処理に基づく通知・措置メカニズムの利用停止を回避するには、正確性の原則の遵守が特に重要である。また、オンラインプラットフォームプロバイダは、DSA 第 23 条の範囲内で実施する可能性のある処理に関してデータ対象者に対して透明性を確保し、GDPR 第 12 条に定められた条件に沿って、GDPR 第 13 条及び第 14 条で要求される情報の全要素を提供することが重要である。加えて、データ最小化原則及びデータ保持期間原則の遵守を慎重に検討すべきである。これにより、明らかに根拠のない通知や苦情の提出を回避する目的に厳密に必要な個人データのみが処理され、かつ想定された目的に必要な期間のみ処理されることが保証される。第 23 条が「合理的な期間」に限り停止を認めている点を考慮すべきである。最後に、欧州データ保護委員会（EDPB）は、アカウントの一時停止が、サービス停止期間中もオンラインプラットフォームプロバイダによって処理され続ける個人データに関するデータポータビリティ権を含む、GDPR に基づくデータ対象者の権利を損なわないことを強調している。

2.3 欺瞞的な設計パターン（第 25 条）

43. DSA 第 25 条(1)は、オンラインプラットフォームプロバイダに対し、サービスの取得者が自律的かつ情報に基づいた意思決定を行う能力を損なわない方法で、オンラインインターフェースを設計・構成・運用することを義務付けている。EDPB の「欺瞞的な設計パターンに関するガイドライン」は、こうしたパターンが「ユーザーのパーソナルデータの処理に関して、意図せず、望まず、かつ潜在的に有害な決定（多くの場合、ユーザーの利益に反し[オンライン]プラットフォームの利益にかなう決定）をユーザーに促そうとするものである」と強調している。欺瞞的な設計パターンはユーザーの行動に影響を与え、個人データを効果的に防御し、意識的な選択を行う能力を阻害する可能性がある。[68]DSA 第 25 条(2)によれば、DSA 第 25 条(1)の禁止規定は、GDPR または指令 2005/29/EC（不公正な商業慣行指令、UCPD）の対象となる慣行には適用されない。欺瞞的なデザインパターンの例は、DSA 67 前文、ソーシャルメディアプラットフォームのインターフェースにおける欺瞞的なデザインパターンに関する EDPB ガイドライン 3/2022 、[69] 、および EU 委員会通知 (2021/C 526/01) 不公正な商業慣行に関する指令 (UCPD) に記載されている。[70]消費者保護・協力ネットワーク

[66]DSA 第 63 項 前文

[67]DSA 第 23 条(1)によれば、オンラインプラットフォームプロバイダは、サービス停止を合理的な期間に限定し、かつ、停止の可能性の理由及び当該決定に対する救済手段を含む事前警告を発出した後にのみ、サービスを停止しなければならない。さらに、DSA 第 23 条(3)は、DSA 第 23 条に基づく停止決定は「個別事例ごとに」行われるべきであることを明確にしている。

[68]EDPB ガイドライン 3/2022「ソーシャルメディアプラットフォームインターフェースにおける欺瞞的な設計パターン：その認識と回避方法」、バージョン 2.0、2023 年 2 月 14 日採択、3 ページ。

[69]EDPB ガイドライン 3/2022「ソーシャルメディアプラットフォームインターフェースにおける欺瞞的設計パターン：その認識と回避方法」、バージョン 2.0、2023 年 2 月 14 日採択。

[70]EU 委員会通知（2021/C 526/01）は、UCPD の解釈と適用に関するガイダンスを提供しており、そのセクション 4.2.7 では「ダークパターン」についても言及している。

（CPC）[71] も、EU の消費者保護法を欺瞞的なデザインパターンに適用する上で関連性のある、ダークパターンに関する調査を実施しました。[72]DSA 第 25 条 (1) が適用される限り、DSA 前文 67 には、欺瞞的なデザインを構成しないものの例が記載されている。すなわち、「例えば広告において、EU 法に準拠した正当な慣行は、それ自体が [欺瞞的なデザイン] パターンを構成するものと見なされるべきではない」とされている。

44. データ保護当局は、GDPR の対象となる欺瞞的な設計パターンに対処する責任を負うが、これはケースバイケースで評価する必要がある。[73] 欺瞞的な設計パターンが GDPR の対象となるか否かを評価する際に考慮すべき重要な要素は、個人データが処理されているかどうか、およびそのパターンが影響を与えているデータ対象者の行動がパーソナルデータの処理に関連しているかどうかである。[74]例えば、「在庫がわずかである」といった（感情的な）誘導によってサービスのすべての取得者に製品購入を促そうとするパターンは、GDPR の対象外となる可能性があります。しかし、「在庫がわずかである。今すぐメールアドレスを入力して予約してください」といった表現によってサービスの取得者が（追加の）個人データを提供するように操作された場合、あるいは本来提供する必要のない個人データを提供した場合、そのパターンは GDPR の対象となる。さらに、サービスの取得者が法人（例：ビジネスユーザー）である場合、そのパターンは GDPR の対象となる。メールアドレスを入力して今すぐ予約」といった手法で、本来提供しないはずの追加個人データを取得させる場合、当該パターンは GDPR の適用対象となる。また、サービスの取得者が法人（例：ビジネスユーザー）である場合、自然人に関連する個人データが処理されない限り、GDPR は適用されない。[75]いずれにせよ、欺瞞的な設計パターンが UCPD または GDPR の適用対象外である場合、DSA 第 25 条(1)が適用され、オンラインプラットフォームプロバイダに対する欺瞞的な設計パターンの明確な一般的禁止を規定している。

45. なお、GDPR 第 5 条(1)(a)に基づくパーソナルデータの処理は、データ対象者に対して合法的、公正かつ透明性をもって行われなければならないため、GDPR が対象とする欺瞞的なデザインパターンの使用 は一般的に違法である。欧州データ保護委員会（EDPB）は「公正性は包括的な原則であり、個人データがデータ対象者にとって有害、差別的、予期せぬ、または誤解を招く方法で処理されてはならない」と指摘している。これは管理者が欺瞞的な設計パターンを展開する場合にしばしば該当する。[76]

46. 欺瞞的な設計パターンの特殊な事例として、「依存性行動を引き起こす可能性」や「サービスの取得者に行動依存症を促進する可能性」のある設計パターンが挙げられ、これらは DSA（デジタルサービス法）の前文 81 および 83 において、システミックリスクの潜在的要因として識別されている。[77]これらのパターンは、ユーザ

---

[71]CPC ネットワーク、https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/consumer-protection-cooperation-network_en。

[72]CPC ネットワーク、https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en#ref-2022--sweep-on-dark-patterns。

[73]EDPB ガイドライン 3/2022「ソーシャルメディアプラットフォームインターフェースにおける欺瞞的な設計パターン：その認識と回避方法」、バージョン 2.0、2023 年 2 月 14 日採択、第 4 項。

[74]第 29 条データ保護作業部会、個人データの概念に関する意見 4/2007、WP 136、2007 年 6 月 20 日採択、10 ページ；参照：欧州司法裁判所判決 2017 年 12 月 20 日 Peter Nowak 対 Data Protection Commissioner, C-434/16, ECLI:EU:C:2017:994, 35 項。([75])

[75]GDPR 第 4 条(1)。

[76]EDPB ガイドライン 3/2022「ソーシャルメディアプラットフォームインターフェースにおける欺瞞的な設計パターン：その認識と回避方法」、バージョン 2.0、2023 年 2 月 14 日採択、特に第 9 項以降；EDPB ガイドライン 4/2019「第 25 条 設計時およびデフォルト時におけるデータ保護」、バージョン 2.0、2020 年 10 月 20 日採択、特に 16 ページ。

[77]「オンラインサービスの『操作的デザイン』、『中毒性デザイン』または『行動デザイン』とは、行動関連のリスクや危害（『過度または有害なインターネット利用』、『スマートフォン依存症』、『技術・インターネット依存症』、『ソーシャルメディア依存症』などの

ーがオンラインプラットフォームの使用に過度に時間を費やすよう促す設計上の特徴、属性、または慣行に依存する可能性がある。こうしたパターンは通常、ユーザーが自由かつ情報に基づいた意思決定を行う能力を欺く、操作する、または実質的に歪める、あるいは損なうことを意図して設計されている。[78] こうした欺瞞的な設計パターンの使用には、個人データの入力が必要となる場合、新たな個人データやプロファイルの収集・生成を伴う場合、あるいは個人データの処理の文脈においてユーザーの行動や意思決定に影響を与える場合がある。

47. 中毒性のある行動を引き起こす可能性のある欺瞞的な設計パターンの一般的な例には、無限スクロール、無限ストリーミング、自動再生、定期的な報酬、ステータスや評判の改善、コレクションの完成、ゲーミフィケーション、カウントダウンタイマーなどが含まれる。[79]こうしたパターンの例は、EDPB の「ソーシャルメディアプラットフォームインターフェースにおける欺瞞的な設計パターンに関するガイドライン」でも説明されており、その目的はとりわけ「ユーザーの感情状態に影響を与え、データ保護上の利益に反する行動を取らせる可能性が高い方法」にある。[80]

2.4 広告の透明性と、特別なカテゴリーのデータを用いたプロファイリングに基づく広告表示の禁止（第 26 条）

48. DSA 第 26 条は、オンラインプラットフォームプロバイダに対する広告に関する透明性規則を定め、オンラインプラットフォームプロバイダが、GDPR 第 9 条(1)で言及される特別なカテゴリーのデータを用いたプロファイリングに基づいて取得者に広告を提示することを禁止している。

49. DSA の 68 項は、DSA 第 26 条の要件が GDPR（特に異議申立権、プロファイリングを含む自動化された個別意思決定に関する規定、およびターゲティング広告のための個人データの処理前にデータ対象者の同意を取得する必要性）を妨げないことを明確にしている。また、e プライバシー指令の規定、特に「端末機器への情報の保存及びそこに保存された情報へのアクセスに関する規定」にも影響を与えない。

2.4.1 広告に関する一般的な透明性義務

50. GDPR 第 13 条及び第 14 条は、個人データが処理される際にデータ対象者に提供すべき情報及びその提供方法を定義している。これらの一般規則は、オンラインプラットフォーム上での広告の文脈で発生し得る処理を含む、あらゆるデータ処理に適用される。

51. DSA 第 26 条(1)は、特に広告に関してオンラインプラットフォームプロバイダに対する透明性規則を定めている。本規定は、各広告に関する情報をサービスの取得者にリアルタイムで提供すべきことを規定している。さらに、広告が表示される取得者を決定するために使用される主要なパラメータに関する有意義な情報、および

デジタル依存症形態を含む）を招く機能を指す」欧州議会決議（2023 年 12 月 12 日採択）「オンラインサービスの依存性設計と EU 単一市場における消費者保護」（2023/2043(INI)）、A 項参照。また、デジタル公平性に関する EU 消費者法の適合性検証を支援する最近の研究及び現代化指令（EU）2019/2161 の適用に関する報告書を参照のこと。

[78]同上

[79]同上

[80]EDPB ガイドライン 3/2022「ソーシャルメディアプラットフォームインターフェースにおける欺瞞的設計パターン：その認識と回避方法」、バージョン 2.0、2023 年 2 月 14 日採択、特にセクション 4.3 を参照。

該当する場合、DSA 第 26 条(1)(d)で規定されるそれらのパラメータを変更する方法に関する情報は、広告から直接アクセス可能でなければならない。

52. これは、DSA 第 26 条で言及される情報の要素はリアルタイムで提供され、広告から直接アクセス可能であるべきである一方、GDPR 第 13 条および第 14 条に定められた透明性義務に関連する情報は、プライバシーポリシー（例：ワンクリックでアクセス可能）を通じて提示される可能性があることを意味する。

53. また、DSA 第 26 条で要求される情報は、パーソナルデータの処理が行われた後に提供される可能性があることも意味する。

54. これは DSA 第 26 条と GDPR の透明性要件との重要な相違点である。後者では、データ対象者から直接収集された個人データの場合、GDPR 第 13 条(1)および(2)に定められる通り、処理が行われる前に、個人データが取得される時点で情報を提供しなければならないと規定している。

55. オンラインプラットフォームプロバイダによる処理の法的根拠（GDPR 第 6 条(1)）にかかわらず、DSA 第 26 条の透明性要件は適用される。

56. さらに、広告目的の処理が同意に基づく場合（GDPR 第 6 条(1)(a)）、処理（プロファイリングを含む）に関する特定の情報は、同意取得前に個人に提供されなければならない。DSA 第 26 条(1)に基づく追加情報（ ）は、その後、広告から直接かつ容易に取得者がアクセス可能となる。

2.4.2 自動化された個別意思決定およびプロファイリングに関する法的枠組み（ ）

57. DSA 第 26 条(1)(d)項によれば、「オンラインインターフェース上で広告を表示するオンラインプラットフォームのプロバイダは、各個別の取得者に提示される各特定の広告について、サービスの取得者が、明確かつ簡潔で誤解を招かない方法で、リアルタイムに[…]、広告から直接かつ容易にアクセス可能な、当該広告が提示される取得者を決定するために使用された主要なパラメータに関する意味のある情報、および該当する場合、それらのパラメータを変更する方法に関する情報を識別できるようにしなければならない」

58. DSA の前文 68 項では、「こうした説明には、広告の提示方法（例：コンテクスト広告かその他の広告か）や、該当する場合の主要なプロファイリング規準に関する情報を含めるべきである。また、取得者がこうした規準を変更できる手段についても通知すべきである」と示されている。

59. GDPR 第 4 条(4)は、プロファイリングを「個人データを用いて自然人に関連する特定の個人的側面を評価する、あらゆる形態のパーソナルデータの処理。特に、当該自然人の業務遂行能力、経済状況、健康状態、個人的嗜好、関心、信頼性、行動、位置情報または移動に関する側面を分析または予測することを目的とするもの」と定義している。

60. 実際、オンラインプラットフォームのユーザー嗜好情報を収集し、それに応じた広告表示を可能とするプロバイダやその他の主体は、GDPR 第 4 条(4)項の定義に基づくプロファイリングを頻繁に実施している。[81]

61. しかしながら、DSA 第 26 条(1)は、プロファイリングを伴わず、より少ない（あるいは全く）個人データの処理を伴う広告形態、例えば一般的な広告にも適用される。

[81] EDPB ガイドライン 8/2020「ソーシャルメディアユーザーのターゲティング」バージョン 2.0（2021 年 4 月 13 日採択）も参照のこと。

62. DSA 第 26 条(1)の広告透明性に関する規定は、事案の特性を考慮した上で、GDPR 第 22 条(1)の規準を満たす自動化された個別意思決定およびプロファイリングの範囲に該当するデータ処理慣行にも関連し得る。[82] ただし、当該プロファイリングが法的効果を伴う決定 を生じさせるか、データ対象者に同等の重大な影響を及ぼす場合に限られる。[83]特定の広告を個人に提示する自動化された決定が法的効果を生じさせるか、または同様に重大な影響を与えるかを評価するには、個人データ処理活動（個々の広告配信レベルを含む）の以下の（網羅的ではない）特徴を考慮すべきである：・プロファイリングプロセスの侵入性・異なるウェブサイト、デバイス、サービス間での個人の追跡・関係する個人の期待と意向広告配信の方法、または標的とされたデータ対象者の脆弱性に関する知識の利用。[84]

63. GDPR 第 22 条(1)項によれば、データ対象者は「自身に法的効果をもたらす、または同様に重大な影響を及ぼす、プロファイリングを含む自動化された処理のみに基づく決定の対象とならない権利」を有する。

64. ただし、契約の履行に必要な場合、EU または加盟国の法令により認められた場合、またはデータ対象者の明示的な同意に基づく場合など、GDPR 第 22 条(2)で定義される特定の法的根拠に依拠する場合には、このような処理は合法となり得る。

65. データが直接的または間接的に取得されたか否かにかかわらず、GDPR は第 13 条及び第 14 条に基づき、データ対象者に対し「第 *22 条(1)*及び*(4)*で言及される自動化された意思決定（プロファイリングを含む）の存在、並びに少なくとも当該ケースにおいては、関連するロジック、当該処理の意義及び想定される結果に関する意味のある情報」について適切に通知することを義務付けている。GDPR の補足条項 71 はさらに、GDPR 第 22 条の範囲内での処理は「適切な保護措置の対象とすべきであり、これにはデータ対象者への具体的な情報提供、人的介入を求める権利、自身の見解を表明する権利、当該アセスメント後に到達した決定の説明を得る権利、および決定に異議を申し立てる権利（…）を含むべきである」と示している。[85] さらに、GDPR の 60 項の前文は「プロファイリングが GDPR 第 22 条の適用範囲外である場合であっても、データ対象者はプロファイリングの存在及びその な結果について通知されるべきである」と述べている。[86]

---

[82]第 29 条データ保護作業部会ガイドライン「自動化された個人に対する意思決定及びプロファイリングに関するガイドライン（規則 2016/679 の目的のため）」（2017 年 10 月 3 日採択、最終改訂・採択：2018 年 2 月 6 日、WP251rev.01、22 ページ）参照。

[83]DSA 第 26 条(1)は、オンラインプラットフォームプロバイダに対し、広告が表示される取得者を決定するために使用される主要なパラメータ、および該当する場合それらのパラメータを変更する方法について透明性を提供することを要求している。本規定は、広告の表示対象者を決定する際にプロファイリングが使用されたか否かについて、オンラインプラットフォームのプロバイダに情報を提供するよう特に要求するものではない。ただし、当該プロファイリングが GDPR 第 22 条(1)に該当する場合、GDPR 第 13 条(2)(f)または第 14 条(2)(g)に基づき当該情報を提供する必要が生じ得る。

[84]EDPB ガイドライン 8/2020「ソーシャルメディアユーザーのターゲティングに関するガイドライン」、バージョン 2.0、2021 年 4 月 13 日採択、24 ページ例 8、85-88 項。参照：第 29 条データ保護作業部会、自動化された個人に対する意思決定及びプロファイリングに関するガイドライン（規則 2016/679 の目的のため）、2017 年 10 月 3 日採択、最終改訂・採択 2018 年 2 月 6 日、WP251rev.01、21-22 ページ。

[85]参照：第 29 条データ保護作業部会、「規則 2016/679 に基づく自動化された個別意思決定およびプロファイリングに関するガイドライン」、2017 年 10 月 3 日採択、最終改訂・採択 2018 年 2 月 6 日、WP251rev.01、第 IV 章（セクション E）、24 ページ。

[86]参照：第 29 条データ保護作業部会、「規則 2016/679 の目的のための自動化された個人決定およびプロファイリングに関するガイドライン」、2017 年 10 月 3 日採択、最終改訂・採択 2018 年 2 月 6 日、WP251rev.01、第 III 章（セクション D）、16 ページ。

66. したがって、DSA 第 26 条で言及されている要素または要素の一部は、特に GDPR 第 22 条が適用される場合、プロファイリングの主要なパラメータに関して、GDPR の下で既にデータ対象者にプロバイダされるべきである。[87]

67. したがって、DSA と GDPR の双方は、オンラインプラットフォームにおける広告配信に関連する透明性義務を包含している。DSA は、関連情報の提供方法や期待される情報・制御の水準（例えば、特定の広告が取得者に提示されることを決定する主要なパラメータの提供、およびそのような変更の可能性がある場合には当該パラメータを変更する可能性に関する情報の提供など）を規定することにより、追加的な義務を定めている。

68. いずれにせよ、GDPR 第 5 条(1)(b)に基づき、個人データの収集は、その処理が広告の提示につながるか否かにかかわらず、特定され、明示的かつ正当な目的のために行われなければならない。

69. パーソナルデータの処理が合法であるためには、GDPR に基づく有効な法的根拠に依拠しなければならない。この処理がプロファイリングを構成するか、広告の提示につながるか、あるいは他の目的を果たすか否かは問わない。

70. 例えば、当該処理が GDPR 第 6 条(1)(a)及び ePrivacy 指令第 5 条(3)に定める同意に基づく場合、同意は GDPR 第 4 条(11)及び第 7 条に規定される全ての規準を満たすことで初めて妥当性とみなされる。[88] 特に、データ対象者は同意を付与したのと同様に容易に、いつでも同意を撤回できる権利を有し、この可能性についても通知されなければならない。

71. 当該処理が正当な利益に基づく場合、[89] データ対象者は GDPR 第 21 条(3)に基づき「ダイレクトマーケティング」目的の処理に対して無条件に異議を申し立てる権利を有する。これにはターゲティング広告の表示（ 商業目的のメッセージをエンドユーザーに直接個別に提示すること）のための処理が含まれるが、[90] これらのターゲティング広告が DSA 第 26 条(3)で既にプロバイダによって禁止されていない場合に限る。

2.4.3 特別な種類のデータを用いたプロファイリングに関する法的枠組み

72. 特別な種類のデータの処理（[91] これに基づくプロファイリングを含む）は、GDPR 第 9 条に定められた特定の法的枠組みの対象となる。原則として、GDPR 第 9 条(2)に定められた特定の例外に依拠しない限り、こ

---

[87]参照：第 29 条データ保護作業部会、「規則 2016/679 の目的のための自動化された個別意思決定およびプロファイリングに関するガイドライン」、2017 年 10 月 3 日採択、最終改訂・採択 2018 年 2 月 6 日、WP251 rev.01、25 ページ「『関与するロジック』に関する有意義な情報」の項。また、欧州司法裁判所判決（2025 年 2 月 27 日）Dun & Bradstreet Austria GmbH 事件（C-203/22、ECLI:EU:C:2025:117）60 項及び 61 項を参照。

[88]EDPB ガイドライン 05/2020（2016/679 規則に基づく同意に関するもの）、バージョン 1.1、2020 年 5 月 4 日採択。

[89]広告における正当な利益に関する欧州司法裁判所判決（2023 年 7 月 4 日 Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537、86 項以降）参照。

[90]2021 年 11 月 25 日付欧州司法裁判所判決 StWL Städtische Werke Lauf a.d. Pegnitz GmbH 対 eprimo GmbH 事件（C-102/20、ECLI:EU:C:2021:954）47 項参照。同判決第 50 項において、欧州司法裁判所は、問題の広告が事前に識別された取得者宛てのものか、あるいは多数の取得者に対して無作為に大量送信されるものかは、問題としない旨も言及している。

[91]GDPR 第 9 条(1)：「人種的・民族的出身、政治的意見、宗教的・哲学的信条、労働組合への加盟を明らかにする個人データ、ならびに自然人を唯一無二に識別する目的での遺伝データ、生体データ、健康に関するデータ、自然人の性生活または性的指向に関するデータの処理」

のような特別な種類のデータの処理は禁止されている。GDPR 第 9 条(1)に基づく特別な種類のデータの範囲は非常に広範である。特に、プロファイリング活動から導出または推論されたデータ（[92] ）や、間接的な開示（[93] ）も含まれる可能性がある。さらに、当該処理操作によって明らかにされる情報が正確であるか否か、また管理者が当該カテゴリーに該当する情報を取得する目的で行動しているか否かは問題ではない（[94] ）。

73. さらに、GDPR 第 22 条の範囲内における自動化された個人に対する意思決定は、当該処理がデータ対象者の明示的な同意（GDPR 第 9 条(2)(a)）に基づく場合、または GDPR 第 22 条(4)に基づき重大な公共の利益のために必要である場合（GDPR 第 9 条(2)(g)）を除き、GDPR 第 9 条(1)で言及される特別なカテゴリーの個人データに基づいてはならない。

74. ただし、DSA 第 26 条(3)によれば、「オンラインプラットフォームのプロバイダは、*EU* 規則 *2016/679* 第 *4* 条*(4)*で定義されるプロファイリングに基づき、*EU* 規則 *2016/679* 第 *9* 条*(1)*で言及される特別な種類の個人データを用いて、サービスの取得者に対して広告を表示してはならない」。

75. これは、GDPR が広告目的で特別なカテゴリーのデータを利用するオンラインプラットフォームによるプロファイリングに関して、特定の例外規定を要求していることを意味する。一方、DSA は、オンラインプラットフォームプロバイダが サービスの取得者に対して、そのような特別なカテゴリーの個人データを用いたプロファイリングに基づく広告を表示することを禁止している。このプロファイリングがオンラインプラットフォームプロバイダ自身によって行われるか、他の者によって行われるかは問いません。

例 2 – 特別なカテゴリーのデータに基づくプロファイリング

ある企業が、地理的位置情報（例：礼拝所の訪問）や購買習慣（例：特定の食品の購入）から推測した宗教的信念を用いて生活様式や購買パターンを予測し、その予測に基づいて広告を提示する。

76. DSA が定めるこれらの特別規則は、適用される場合には、GDPR 第 9 条(2)および第 22 条(4)に定められた規則を補完するものである。オンラインプラットフォームプロバイダが、サービスの取得者に対して、特別なカテゴリーの個人データを用いたプロファイリングに基づく広告を表示することは、オンラインプラットフォームプロバイダまたは他の事業体が、この処理について GDPR 第 6 条(1)に基づく適切な法的根拠および GDPR 第 9 条(2)に基づく適切な例外規定に依拠する場合であっても、DSA により禁止される。

2.4.4 広告透明性義務から生じるデータの安全性及び機密性

77. DSA 第 26 条(1)(d)は、各広告が表示される取得者を決定するために使用される主要なパラメータに関する情報をプロバイダが提供しなければならないと規定している。DSA の前文 68 項によれば、「サービスの取得者は、広告が表示されるオンラインインターフェースから直接アクセス可能な形で、特定の広告が自身に表示されることを決定するために使用される主要なパラメータに関する情報を得るべきであり、その目的のために使用されるロジック（プロファイリングに基づく場合を含む）について意味のある説明が提供されるべきである」。実際には、この情報は、ユーザーの推定される嗜好や過去の閲覧履歴を明らかにする可能性があるため、個人情報に該当するケースが多いと考えられる。

[92]欧州司法裁判所 2023 年 7 月 4 日付判決 Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537、第 73 項。

[93]欧州司法裁判所判決 2022 年 8 月 1 日 OT 及びリトアニア事件 C-184/20, ECLI:EU:C:2022:601.

[94]欧州司法裁判所 2023 年 7 月 4 日付判決 Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537、69 項。

78. DSA の前文 107 で想起されるように、「オンライン広告の提供には通常、広告主と広告掲載者を結びつける仲介サービスを含む複数の主体が関与する」当該情報がサービスの取得者に到達するためには、これらの仲介事業者が情報伝達を促進する必要がある。情報の提示および（そのような可能性が存在する場合には）パラメータ変更の機能が、いかなる仲介事業者もサービスの取得者に関する追加情報にアクセスまたは収集することを可能としないよう、適切な技術的・組織的措置を実施しなければならない。関連する処理は、GDPR 第 32 条の義務、GDPR 第 5 条(1)(c)に基づくデータ最小化、および GDPR 第 25 条に基づく設計時およびデフォルト時のデータ保護を遵守すべきである。DSA 第 26 条に定める透明性義務の遵守は、仲介業者への個人データの追加共有を伴うべきではない。仲介企業を通じたサービス取得者に関する情報のアクセスまたは収集には、GDPR 第 6 条に基づく適切な法的根拠が必要であり、GDPR 第 5 条に定める原則を遵守しなければならない。

79. さらに、仲介サービスプロバイダは、可能な範囲でかつ個人データの収集増加を招くことなく、当該プロファイリングの対象となる単一のサービス取得者に対してのみ情報が提供されるよう、適切な措置を講じるべきである。

2.5 レコメンダーシステム（第 27 条及び第 38 条）

80. DSA 第 3 条(s)で定義される「レコメンデーションシステム」とは、オンラインプラットフォームが特定の相対的順序や目立ち度でプラットフォーム利用者に特定のコンテンツを提示するために使用する、部分的または完全な自動化システムである。オンライン検索エンジンも、ユーザーに検索結果を提案する際に推薦システムを利用する場合がある。[95] これらのシステムは、取得者にとって情報へのアクセスを促進・最適化する有用性から、今日のオンラインプラットフォームで広く普及している。DSA は、コンテンツの拡散・バイラル化やオンライン行動の促進における推薦システムの重要な役割を認識している。[96] DSA はまた、ユーザーをエンパワーメントするため、第 27 条及び第 38 条に特定の保護措置を導入している。

81. 膨大なコンテンツカタログを有するオンラインプラットフォームのプロバイダは、通常、自社のウェブサイトのランディングページやアプリのフィード、あるいはユーザーにコンテンツを提示するサービスのその他の機能を通じて、特定のコンテンツを最初に、あるいは目立つ形でユーザーに提案したいと考える。これは、そうでなければ膨大な数のコンテンツ項目がユーザーを圧倒し、サービスの継続利用を妨げる可能性があるためである。コンテンツの選択と提示順序は、通常、オンラインプラットフォームのプロバイダが定義した規準に基づくものであり、プラットフォームが配信可能な全コンテンツの中から行われる推奨を構成する。この推奨活動には、フィルタリング、ランキング、その他の優先順位付けロジックの適用が含まれ、多くの場合パーソナライズされ、ユーザーの関心を最も引きそうなものを最初に提示すること、あるいはユーザーに提示されるコンテンツの質や多様性を高めることを目的とする。レコメンデーションシステムはパーソナルデータの処理を伴う場合もあるが、そうでない状況も存在する。例えば、EC サイトプロバイダがホームページにアクセスした顧客に対し、最初にベストセラー商品を提案することを決定する場合が挙げられる。この場合、サービスを利用するユーザーの特定の特性を認識せずに推薦が行われ、その基盤となる推薦プロセスはパーソナルデータの処理を一切伴わない。

82. しかしながら、現実のシナリオでは、コンテンツ提示のパーソナライズ化と効率化を目的とした自動化された個人データの処理がますます増加している。ユーザーに表示するアイテムを選択する際、レコメンデーションシステムのアルゴリズムは通常、ユーザーの行動に関するデータを処理し、他のユーザーの行動データ（ ）を基に、

[95]デジタルサービス法（DSA）第 3 条(s)項及び(j)項参照。

[96]DSA 前文第 70 項参照。

どのアイテムがユーザーの関心をより引きつけ、コンテンツとの関与を促す可能性が高いかを予測することもできる。[97]

83. 個人データの処理により、プロバイダは効率的で精度の高いレコメンデーションシステムをオンラインプラットフォームに組み込むことが可能となる一方で、これらのシステムが対象となるデータ対象者にとってリスクを伴うことも強調すべきである。[98] こうしたリスクの一部は、個人データの大規模な処理、推論や個人データの組み合わせに関する正確性・透明性の潜在的な欠如、評価やスコアリング（プロファイリング）、および特別なカテゴリーのデータ、高度に個人的な性質を持つデータ、脆弱なデータ対象者のデータの処理に関連している。[99]

84. GDPR によれば、予測目的の行動分析は「個人データを用いて自然人に関連する特定の個人的側面を評価すること、特に当該自然人の（…）個人的嗜好、関心、（…）行動に関する側面を分析または予測すること」を伴うため、プロファイリング活動に該当する。[100] レコメンデーションシステムにおける個人データの処理は、合法性・公正性・透明性の原則、目的限定の原則、正確性の原則を含む GDPR の適用対象となる。[101] この文脈でデータ対象者をプロファイリングするための GDPR 第 6 条(1)に基づく適切な法的根拠の確保、および（該当する場合）特別カテゴリーのデータが関与する場合には GDPR 第 9 条(2)に基づく例外規定の適用が特に重要である。また、オンラインプラットフォームのユーザーに対しレコメンダーシステムを通じて特定のコンテンツを提示する行為が、GDPR 第 22 条(1)の意味における「決定」、すなわちデータ対象者に重大な影響を及ぼす決定に該当する可能性を排除できない点も強調すべきである。この文脈において、「決定」は「データ対象者に様々な形で影響を与え得る一連の行為を含む広範な概念」と捉えるべきである（[102]）。この点を踏まえると、オンラインプラットフォームのユーザーに対しレコメンダーシステムを通じて特定のコンテンツを提示する過程で行われる個人データの処理が、特に個人に重大な結果をもたらし得る場合には、GDPR 第 22 条に基づく自動化された決定（）に該当する可能性を排除できない（[103]）。

---

[97] これは「協調フィルタリング」と呼ばれる。Schafer, J.B., Frankowski, D., Herlocker, J., Sen, S. (2007).Collaborative Filtering Recommender Systems. In: Brusilovsky, P., Kobsa, A., Nejdl, W. (eds) The Adaptive Web. Lecture Notes in Computer Science, vol 4321. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-720799_9.

[98] DSA 第 70 項。

[99] 参照：第 29 条データ保護作業部会ガイドライン「データ保護影響評価（DPIA）および処理が『高いリスクをもたらす可能性が高い』かどうかを判断するための規準の決定について」、WP 248 rev.01、2017 年 10 月 4 日、p. 9 ff.

[100] GDPR 第 4 条(4)。

[101] GDPR 第 4 条(4)及び第 5 条参照。

[102] C-634/21 OQ 対 ヘッセン州事件におけるピカマエ司法顧問の意見書（2023 年 3 月 16 日提出、ECLI:EU:C:2023:220）、38 項；欧州司法裁判所判決（2023 年 12 月 7 日 OQ 対 ヘッセン州、C634/21、ECLI:EU:C:2023:957）、44-46 項。特に第 45 項において、裁判所は「『決定』という概念の広範な範囲は、*GDPR* の前文 *71* によって確認されている。それによれば、個人に関連する個人的側面を評価する決定（当該個人がその対象となることを拒否する権利を有するべきものである）は、『当該個人に関する法的効果を生じさせる』措置、あるいは『同様に当該個人に重大な影響を及ぼす』措置を含む場合がある」と判示した。

[103] 2016/679 規則に基づく自動化された個別意思決定及びプロファイリングに関する第 29 条データ保護作業部会ガイドライン（最終改訂・採択：2018 年 2 月 6 日、21 ページ）は、「データ処理が個人に重大な影響を及ぼすためには、処理の影響が注目に値するほど十分に大きく、または重要でなければならない。言い換えれば、当該決定は次の可能性を有していなければならない：

- ・関係者の状況、行動、選択に重大な影響を与えること；
- データ対象者に長期または恒久的な影響を与えること；または

85. 特に、レコメンダーシステムがデータ対象者に重大な影響を及ぼす結果をもたらす推奨を提示する場合、すなわち特定のコンテンツを個人に提示するという「決定」が、必ずしも法的ではなく経済的・社会的な影響を及ぼす可能性がある場合に、このケースが該当し得る。[104]特に注意を払うべきは、アルゴリズム処理が個人に長期的または恒久的な影響を与えるコンテンツ・サービス・製品を提案したり、行動や選択に重大な影響を及ぼしたりするケースである。例としてオンラインプラットフォーム上の住宅・求人オファー向け推薦システムが挙げられる。DSA はレコメンダーシステムに関連するデータ対象者の影響を強調し、「レコメンダーシステムは、サービス取得者が関連情報を検索しやすくし、ユーザー体験の向上に寄与するなど、オンライン情報へのアクセス・相互作用能力に重大な影響を与え得る。また特定のメッセージの拡散、情報のバイラルな伝播、オンライン行動の促進においても重要な役割を果たす」と述べている。[105]

86. オンラインプラットフォームのプロバイダは、GDPR に基づき、自社のサービスに組み込むことを決定したレコメンダーシステムによって処理される個人データに関して、データ管理者として行動する。他の関連する GDPR 規定を全て遵守する必要性に加え、プロバイダは特に、GDPR 第 12 条、第 13 条及び第 14 条（GDPR 第 22 条(1)が適用される場合には第 13 条(2)(f)及び第 14 条(2)(g)を含む）の要件に沿い、レコメンデーションシステムにおける個人データの処理に関して適切な透明性義務を履行しなければならない。[106]同様に、欧州データ保護委員会（EDPB）は、デジタルサービス法（DSA）第 27 条が、オンラインプラットフォームプロバイダに対し、サービスに組み込む推薦システムで使用される主要パラメータについて 、ユーザーに対して透明性を確保することを義務付けていること、また複数の選択肢が利用可能な場合、サービス取得者がいつでも推薦システムで使用される主要パラメータの優先オプションを選択・変更できる機能を提供することを求めていることを歓迎する。特に、プロバイダは利用規約において、理解しやすい形式で「特定の情報が提案される理由」または優先される理由、特定の順序や情報の目立ち度で表示される理由を明示し、提案に影響を与える主要なパラメータを提示しなければならない。オンラインプラットフォームプロバイダがユーザーに複数の推薦システムオプションを提供する場合には、プロバイダはユーザーが受け取る推薦について一定の制御権を持たせるため、オプション変更機能を提供しなければならない。これらのオプションは、推奨が表示されるオンラインインターフェースから容易にアクセス可能であるべきである。[107]

87. DSA 第 38 条は特に VLOP および VLOSE のプロバイダに適用され、DSA 第 27 条に加えて適用される。DSA 第 38 条によれば、当該プロバイダは、GDPR で定義されるプロファイリングに基づかない推奨システムを、少なくとも 1 つずつ提供しなければならない。[108]欧州データ保護委員会（EDPB）はこの規定を歓迎し、

- 最も極端な場合、個人の排除または差別につながる」

[104]2023 年 3 月 16 日付、C-634/21 OQ 対 ヘッセン州事件におけるピカマエ司法顧問の意見書、ECLI:EU:C:2023:220、パラグラフ 38。

[105]DSA（デジタルサービス法）の理由 70 前文を参照。

[106]これは、処理が GDPR 第 22 条(1)項に該当する場合、「データ対象者に対し、当該活動に従事していることを通知すること；関与するロジックについて意味のある情報をプロバイダすること；および処理の意義と想定される結果を説明すること」を意味する。(...)「自動化された意思決定およびプロファイリングが第 22 条(1)項の定義を満たさない場合でも、上記の情報を提供することは良い慣行である。いずれにせよ、データ管理者は、処理を公正なものとし、第 13 条および第 14 条のその他の情報要件をすべて満たすために、データ対象者に十分な情報をプロバイダしなければならない」。2016/679 規則を目的とした自動化された個別意思決定およびプロファイリングに関する第 29 条データ保護作業部会ガイドライン（2018 年 2 月 6 日に最終改訂・採択）25 ページを参照のこと。

[107]DSA 第 27 条(3)。

[108]DSA 第 9 項（前文）によれば、「大規模オンラインプラットフォーム及び大規模オンライン検索エンジンのプロバイダは、そのサービスの取得者が、推奨システムの主要パラメータについて、EU 規則 2016/679 の意味におけるプロファイリングに基づか

オンラインプラットフォームプロバイダがユーザーに異なる推奨システムオプションを提供するにあたり、GDPR 第 5 条(1)(c)および第 25 条に基づくデータ最小化の原則ならびに設計時およびデフォルト時におけるデータ保護の要件を尊重すべきであることを改めて指摘する。したがって、VLOP および VLOSE のプロバイダは、両方の選択肢を（サービス初回利用時に）平等に提示し、サービスの取得者がプロファイリングに基づく推薦システムを選択するよう誘導してはならない。[109] VLOP および VLOSE のプロバイダは、サービスの取得者がこのオプションを選択した場合にのみ、プロファイリングに基づく推薦システムを使用できる。さらに、非プロファイリングベースのオプションが有効な間は、オンラインプラットフォームプロバイダは、将来のレコメンデーション（例：ユーザーがプロファイリングベースのオプションを選択した場合に備えるため、またはより詳細なプロファイリングに基づくため関連性の高いレコメンデーションを提供するため）を目的として、ユーザーの個人データを収集・処理し続けることは法的に認められない。さらに、ユーザーがプロファイリングに基づくバージョン（ ）とプロファイリングに基づかないバージョンの両方を、例えば 1 日に複数回切り替えて利用する場合、プロファイリングに基づかないバージョン利用中は当該ユーザーのプロファイリングを行ってはならない。

88. DSA 第 27 条および第 38 条は、自然人、オンラインプラットフォームおよび検索エンジンの利用者に対する具体的な保護措置を定めているが、これらの保護措置は個人データのさらなる処理を伴う。したがって、欧州データ保護委員会（EDPB）は、レコメンデーションシステムのパラメータ変更に関連するユーザーの選択の収集および処理は、オンラインプラットフォームおよび検索エンジンのプロバイダが DSA 遵守を唯一の目的として処理し、必要な期間のみ保存すべきであると強調する。プロバイダは過去の選択履歴も保持すべきではない。

2.6 未成年の防御（第 28 条）

89. DSA の目的の一つは、オンライン上における未成年者の保護である。この目的に沿い、DSA 第 28 条は「未成年者がアクセス可能なオンラインプラットフォームのプロバイダは、自らのサービスにおいて、未成年者のプライバシー、安全、セキュリティの高水準を確保するため、適切かつ均衡のとれた措置を講じなければならない」と規定している。さらに、「オンラインプラットフォームの提供者は、サービスの取得者が未成年者であると合理的な確信をもって認識している場合、サービスの取得者の個人データに基づくプロファイリング[…][110] に基づいて、そのインターフェース上に広告を表示してはならない」DSA 第 28 条(3)は、こうした義務の遵守に関して、オンラインプラットフォームプロバイダに、「サービスの取得者が未成年者であるか否かを評価するために追加の個人データを処理する義務」はないと付記している。

90. 未成年者に対する高度なプライバシー、安全及びセキュリティの提供のため、第 28 条に基づき要求される要件として DSA に基づき、オンラインプラットフォームプロバイダは、自社のサービスが未成年者に及ぼす可能性のあるリスク（有害・違法コンテンツへのエクスポージャー、プライバシーリスク、健康・福祉へのリスク、先端技術によるリスク等）を理解し、これらのリスクに対応する技術的・組織的措置を最も適切かつ効果的な方法

ない代替選択肢を常に享受できるよう確保すべきである。かかる選択肢は、推奨が表示されるオンラインインターフェースから直接アクセス可能であるべきである」。

[109]参照：EDPB ガイドライン 4/2019「第 25 条 設計時及びデフォルト時のデータ保護」バージョン 2.0（2020 年 10 月 20 日採択）、19 ページ例 1：VLOP または VLOSE のプロバイダは、「選択肢を提示する際に、データ対象者がデータ管理者に対して収集を許可する方向に誘導するような方法（選択肢が平等かつ中立な方法で提示された場合よりも多くの個人データの収集を許可する方向に誘導する方法）で提示してはならない。これは、データ対象者が自身のデータ共有を拒否することを困難にしたり、データ対象者がプライバシー設定を調整して処理を制限することを困難にするような方法で処理オプションを提示してはならないことを意味する」

[110]GDPR 第 4 条(4)項に定義される通り。

で適応させるべきである。未成年者のプライバシー、安全、セキュリティの高水準を確保するための措置（例：未成年者保護標準の採用、行動規範への参加、年齢確認、ペアレンタルコントロール、不正利用通報ツールなど）が個人データの処理を伴う場合、データ管理者は個人データ処理の必要性と比例性を評価する必要がある。オンラインプラットフォームのプロバイダは、（追加的な）個人データの処理以外の手段によって、自社のサービスが未成年者に利用されていることを認識できる場合がある。例えば、「利用規約で未成年者のサービス利用を許可している場合、サービスが未成年者を対象としている場合、または（サービス上で推進される特定の機能やコンテンツにより）主に未成年者が利用している場合、あるいはプロバイダがサービスの取得者の一部が未成年者であることを何らかの形で認識している場合（例：他の目的で既にサービスの取得者の年齢を明らかにするためのパーソナルデータの処理を行っている場合）」[111] 。

91. DSA 第 28 条(1)で定められるように、個人データの処理なしに未成年者のプライバシー、安全、セキュリティの高水準を確保する可能性はあるものの、DSA 第 28 条(1)は、処理が GDPR の一般的な要件に準拠している限り、個人データの処理を禁止するものではない。さらに、EU データ保護法の観点からは、オンラインプラットフォームプロバイダは、すべての利用者（未成年者だけでなく）に対して、特に処理のリスクに見合った高水準のプライバシー、安全性、セキュリティを確保すべきである。このアプローチは、サービスプロバイダが、サービスの取得者が未成年者であるかどうかを合理的な確実性をもって判断するために（追加の）個人データを処理しない場合にも適用される。

92. GDPR はパーソナルデータの処理に法的根拠を要求する。DSA 第 28 条(1)項及び(2)項は、プロバイダが非常に異なる状況下で遵守すべき義務を規定しており、したがって、そのような義務を遵守するためにパーソナルデータを処理する場合、データ管理者は各事例の特性を考慮し、その合法的な処理を確保しなければならない。[112]この文脈において、DSA 第 28 条(1)項及び(2)項は、GDPR 第 6 条(1)(c)に基づくパーソナルデータの処理の法的根拠となり得る。ただし、データ管理者が（ケースバイケースで）当該処理（例：年齢確認の文脈における処理）が DSA 第 28 条(1)項及び(2)項で定められた目的を達成するために必要かつ比例的であることを立証できる場合に限る。いずれにせよ、DSA 第 28 条(3)は、オンラインプラットフォームプロバイダが、サービスの取得者が未成年者であるか否かを評価するために、追加の個人データを処理（収集及び保存を含む）する義務を負わないことを明確にしている。[113]GDPR 第 6 条(1)(c)に基づく処理は、追求される正当な目的に対して（実証可能な）必要性と比例性を有していなければならない。すなわち、目的達成に同等の効果を持ちながら、より侵襲性の低い代替手段が存在してはならない。[114]GDPR 第 9 条(1)に該当するデータの処理に関しては、管理者はケースバイケースで、GDPR 第 9 条(2)に規定される例外のいずれかに依拠できるかどうかを評価しなければならない。ただし、特に児童のデータが処理されることが予想される場合には、自然人を唯一無二に識別する目的（ ）での生体データなど、特別なカテゴリーのデータの処理は避けるべきである。

---

[111]DSA（データ保護法）前文第 71 項

[112]欧州委員会参照、「規則（EU）2022/2065 第 28 条(4)に基づく、未成年者のオンライン上における高い水準のプライバシー、安全及びセキュリティを確保するための措置に関する委員会ガイドライン、C(2025) 4764 final、https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors で入手可能。

[113]DSA 第 28 条(3)及び前文 71 項。本規定は、GDPR 第 5 条(1)(c)に基づくデータ最小化の原則の精神にも沿うものである。これは、オンラインプラットフォームプロバイダが実施するアセスメントの評価結果を扱う際に特に考慮すべき点であり、例えばプロバイダは取得者の年齢または年齢層を保存すべきではない。

[114]欧州司法裁判所 2023 年 11 月 9 日付判決 Gesamtverband Autoteile-Handel eV 対 Scania CV AB、C319/22 ECLI:EU:C:2023:837、52～62 項。

93. 欧州データ保護委員会（EDPB）は、プラットフォームによる利用者本人の識別なしに年齢確認を実施することも可能であるとの見解を示している。[115] したがって、オンラインプラットフォームプロバイダは、特に DSA 第 28 条のみを根拠として、利用者（例：政府発行の身分証明書による本人確認書類の提出を求めるなど）をオンライン上で明確に特定可能な年齢確認メカニズムを避けるべきである。

94. オンラインプラットフォームプロバイダがアセスメントを実施した結果、自社のプラットフォームにおいて年齢確認が必要であると結論付けた場合、未成年者がプラットフォームにアクセスできないことを確保し、サービスのすべての取得者に対する潜在的な悪影響を防止するためには、リスクベースのアプローチを採用しなければならない。これには、利用者の年齢を推定または確認するために必要かつ比例的な範囲に限定して利用者の個人データの処理することも含まれる（例：年齢範囲がサービスの取得者が未成年者であるという合理的な確実性を提供する場合には、正確な生年月日を検証すべきではない）。[116] さらに、オンラインプラットフォームプロバイダは、年齢確認プロセスを通じてサービスの取得者の年齢または年齢範囲を推定・検証し恒久的に保存すべきではなく、単にサービス取得者がサービス利用条件を満たしているか否かを記録するに留めるべきである。これにより、データ最小化の原則および設計時・デフォルト時におけるデータ保護の原則が実施される。[117]

95. プロバイダが VLOP に指定されたオンラインプラットフォームを運営する場合は、DSA 第 5 条に基づく義務（DSA 第 34 条及び第 35 条の義務を含む）も適用される。[118] この場合、プロバイダは自社のサービスに起因するシステム的リスクの評価を実施し、必要に応じて当該リスクの緩和のための適切な措置を実施しなければならない。DSA 第 35 条(1)(j)によれば、未成年者保護のためのリスク緩和策としては、「児童の権利保護を目的とした対象を絞った措置（年齢検証やペアレンタルコントロールツール、未成年者が虐待を通報したり支援を得たりするためのツールを含む）」が挙げられる。DSA 第 28 条及び第 35 条の要件を GDPR と併せて解釈すると、例えば未成年者へのリスクに応じて年齢確認を実施すべきであり、パーソナルデータの必要かつ比例的な処理を考慮しつつ、特に当該措置がサービスの取得者の基本的権利に与える影響を慎重に検討する必要がある。したがって、プロバイダが、サービスの取得者としての未成年者（ ）に影響するリスクが低いと判断し、かつ、オンラインプラットフォームのプロバイダがユーザーが未成年者であることを合理的な確信をもって認識できる他の手段が実証的に存在しない場合、[119][120]ユーザーが関連する年齢基準を超えていることの確認を求めること、疑義が生じた場合には追加確認を実施すること、あるいはサービスが未成年者によって利用されているか否かにかかわらず全てのユーザーに利益をもたらす措置を講じることが十分である可能性がある。必要な比例原則に基づく措置の必要性及びその内容は、必ずしも DSA や GDPR

[115]例：ゼロ知識証明などのプライバシー保護技術、あるいは技術水準に応じたその他の技術。欧州デジタル身分証明書規則（eIDAS 2.0）の序文 14 項参照。同項では「年齢」が付属書 VI の属性最小限リストに含まれている。低リスクの状況では、生年を提供したり、フォームに記入したりすることが適切である可能性があるが、そのような措置はすべてのケースで完全ではないかもしれない。2020 年 5 月 4 日に採択された、規則 2016/679 に基づく同意に関する EDPB ガイドライン 05/2020、バージョン 1.1、パラグラフ 135 を参照。

[116]年齢確認に関する EDPB 声明 1/2025（2025 年 2 月 11 日採択）も参照のこと。特にセクション 2.2 を参照。

[117]GDPR 第 5 条(1)(c)項及び第 25 条。

[118]本ガイドライン第 2.7 項も参照のこと。([119])

[119]参照：第 91 項。

[120]参照：EDPB ガイドライン 05/2020「規則 2016/679 に基づく同意」（バージョン 1.1、2020 年 5 月 4 日採択）、第 135 項：「疑義が生じた場合、管理者は当該事例における年齢確認メカニズムを見直し、代替的な検証が必要かどうかを検討すべきである」。

（[121]）から導かれるものではなく、例えばEU法や加盟国法の他の手段（[122]）からも導かれる可能性がある。いずれにせよ、GDPRはパーソナルデータの処理に関連して、適切かつ比例的な年齢確認メカニズムが考慮すべき要件を定めている。[123]

96. 年齢確認の文脈におけるパーソナルデータの処理に関するさらなる考察については、EDPBの年齢確認に関する声明を参照のこと。[124]

2.7 リスクアセスメントと緩和（第34条及び第35条）

97. DSA第34条及び第35条は、VLOP（仮想オンラインプラットフォーム）及びVLOSE（仮想オンラインサービス）のプロバイダに、システミックリスクの管理を義務付けている。DSAはシステム的リスクを定義していない。ただし、DSA第34条(1)は、システム的リスクの評価には以下を含めるべきことを明確にしている：a)違法コンテンツの拡散、b)基本権（憲章第7条及び第8条、すなわちプライバシー及びデータ保護に関する基本権を含む）の行使に対する実際的または予見可能な悪影響、c) 市民的議論及び選挙プロセス[125]、並びに公共の安全に対する実際のまたは予見可能な悪影響、ならびに d) 性別に基づく暴力、公衆衛生及び未成年者の保護に関連する実際のまたは予見可能な悪影響、並びに個人の身体的・精神的健康に対する深刻な悪影響。[126] VLOPs および VLOSEs におけるシステミックリスクは、個々のユーザーに限定されない広範な 経済的・社会的・政治的損害を引き起こす可能性があり、同時に個々のユーザーにも影響を及ぼし得る。

98. DSA 第 34 条(2)は、システム的リスクに影響を与えると想定される要素の非網羅的リストを規定しており、これにはプロバイダのレコメンデーションシステム、コンテンツモデレーションシステム、利用規約とその執行、広告、データ関連の実践が含まれる。[127]さらに、サービスの意図的な操作や違法コンテンツの拡散もアセスメントの対象となる。これらの要素は通常、パーソナルデータの処理と関連しているか、それによって初めて可能となるため、GDPRの要件を満たす必要がある。この文脈で特に重要なのは、ソーシャルメディアユーザーへのターゲティングに関するEDPBガイドラインおよび欺瞞的設計パターンに関するEDPBガイドラインである。[128]

---

[121]例：GDPR第8条及び第24条。

[122]例：2018年11月14日付欧州議会及び理事会指令(EU) 2018/1808（市場実態の変化を踏まえ、加盟国における視聴覚メディアサービス提供に関する法令・規制・行政措置の調整を定めた指令 2010/13/EU を改正するもの）第28b 条(3)(a)（市場実態の変化を踏まえた映像メディアサービス指令改正）PE/33/2018/REV/1、OJ L 303、2018年11月28日、69–92頁。

[123]例：GDPR第25条。

[124]年齢確認に関する欧州データ保護委員会声明 1/2025、2025年2月11日採択。

[125]欧州委員会、「委員会、選挙におけるオンライン上のシステミックリスクの緩和のための DSA ガイドラインを公表」、https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707、2024年3月26日。

[126]DSA 前文 80～83 項参照。

[127]これには、DSAの序文79項によれば、サービスが設計される方法（多くの場合広告主導のビジネスモデルに利益をもたらすように）も含まれる。

[128]ソーシャルメディア利用者のターゲティングに関する EDPB ガイドライン 8/2020（バージョン 2.0）、2021年4月13日採択；ソーシャルメディアプラットフォームインターフェースにおける欺瞞的設計パターン：その認識と回避方法に関する EDPB ガイドライン 3/2022（バージョン 2.0）、2023年2月14日採択。

99. リスクアセスメントの一部は、DSA 第 34 条(1)(b)に基づき、基本権の行使に対する実際のまたは予見可能な負の影響（特に基本権憲章第 1 条、第 7 条、第 8 条、第 11 条、第 21 条、第 24 条及び第 38 条を含む）に関するシステミックリスクの評価である。[129]このようなリスクの特定の原因については、DSA の前文 81 でさらに詳述されている。例えば、アルゴリズムシステムの設計に関連して、ケースバイケースでのアセスメント後に必要に応じて[130] 調整すべきであり、特に GDPR 第 9 条に基づく特別なカテゴリーのデータが処理される場合、脆弱な立場にある個人に対する差別につながるバイアスを防止または最小化する措置を講じることで対応できる。[131]こうした潜在リスクへの対応策としては、GDPR 第 25 条に基づく設計時およびデフォルト時のデータ保護の適切な実施、ならびに DSA 第 35 条(1)(d)の緩和措置の採用が考えられる。個人データ保護という基本的権利に影響を及ぼすシステム的リスクが、かつ個々のユーザーに限定されない場合には、GDPR 第 35 条に基づくデータ保護影響評価（DPIA）の実施が義務付けられる可能性が高い。[132] いずれの場合も、当該処理が第 29 条データ保護作業部会ガイドライン（DPIA に関する）の規準のうち 2 つ以上を満たすかどうかを評価すべきであり、場合によっては、データ管理者はこれらの規準のうち 1 つのみを満たす処理についても DPIA が必要と判断できる。[133]さらに、GDPR は特に第 5 条、第 22 条、第 24 条、第 25 条および前文 71・75 に基づき、個人データの処理が合法性、公正性、透明性に従い、差別なく行われることを要求していることに留意すべきである。[134]

100. システム的リスクの緩和策として、DSA 第 35 条では VLOP および VLOSE プロバイダが適用可能な模範的措置のリストを規定している。いずれにせよ、DSA 第 35 条(1)は、特定されたシステム的リスクの緩和のために、措置が合理的、比例的かつ効果的であることを要求している。本節の残りの部分では、GDPR に直接関連する措置について述べるが、他の措置が GDPR に準拠して実施される必要がないことを意味するものではない。

101. 例として、DSA 第 35 条(1)(f)は、有効性を実証するのに特に有用となり得る内部プロセス、リソース、テスト、文書化、監督を列挙している。さらに、DSA 第 35 条(1)(f)は、特にシステミックリスクの検知に関して、これらの措置を強化する可能性に関わっている。これは「設計段階からのデータ保護」の概念の中核でもある（[135]）。また、GDPR 第 25 条に関する欧州データ保護委員会（EDPB）ガイドラインは、この要件を、例えば主要業績評価指標（KPI）や有効性評価の根拠によって補完している。こうした措置はアプリケー

[129]欧州連合基本権憲章、OJ C 326、2012 年 10 月 26 日、p. 391−407。憲章第 8 条には個人データの保護に関する基本的権利が規定されている。

[130]デジタルサービス法（DSA）第 35 条(1)を参照。

[131]DSA 前文第 94 項参照。

[132]十分に包括的な DPIA の規準については、2017 年 10 月 4 日付 WP 248 rev.01「データ保護影響評価（DPIA）に関する第 29 条データ保護作業部会ガイドライン」および規則 2016/679 の目的上「高いリスクをもたらす可能性が高い」処理の規準判定を参照のこと。

[133]同上 p. 9 ff. 規準は「評価またはスコアリング」、「法的または同等の重大な影響を伴う自動化された意思決定」、「体系的な監視」、「機微なデータまたは高度に個人的な性質のデータ」、「大規模に処理されるデータ」、「データセットのマッチングまたは結合」、「脆弱なデータ対象者に関するデータ」、「革新的な利用または新たな技術的・組織的ソリューションの適用」、および処理自体が「データ対象者が権利を行使したり、サービスや契約を利用することを妨げる」場合である。

[134]参照：EDPB ガイドライン 4/2019「第 25 条 設計時及びデフォルト時におけるデータ保護」バージョン 2.0、2020 年 10 月 20 日採択、特に 69 項以降；参照：欧州司法裁判所判決 2023 年 12 月 7 日、OQ 対ヘッセン州、C-634/21、特に 69 特に 69 項以降参照。欧州司法裁判所判決（2023 年 12 月 7 日、OQ 対ヘッセン州、C-634/21、ECLI:EU:C:2023:957）特に 59 項及び 66 項参照。

[135]EDPB ガイドライン 4/2019（第 25 条「設計時およびデフォルト時におけるデータ保護」、バージョン 2.0、2020 年 10 月 20 日採択）、パラグラフ 13 以降、特にパラグラフ 16。

ションの運用段階でも必要であり、開発段階に限定されない点に留意すべきである。GDPR 第 32 条(1)(d)によれば、処理の安全性を確保するための技術的・組織的措置の有効性を定期的にテスト・アセスメントするプロセスが含まれる。また GDPR 第 33 条及び同条第 87 項の前文によれば、準拠した運用からの逸脱が違反を引き起こしたかどうかを判断するための適切な措置が含まれる。

102. DSA 第 35 条(1)(a)は「サービスの設計、機能または動作（オンラインインターフェースを含む）を適応させる」という緩和措置を詳述しており、これは GDPR 第 25 条に基づくデータ保護を設計段階およびデフォルトで組み込む要件に従い、パーソナルデータの処理システムを設計するデータ管理者の義務と重複する。違法コンテンツや違法行為を検知する（自動化された）ツール、[136] 、レコメンデーションシステム、広告システムなどから生じうるシステミックリスクに関しては、データ最小化や擬似匿名化などの技術的・組織的措置を含む GDPR の原則と保護措置を遵守することで、超大規模オンラインプラットフォームおよび超大規模オンライン検索エンジンのプロバイダは、DSA 第 35 条を含む DSA の要件を効果的に遵守することが可能となる。[137] ここで留意すべきは、DSA 第 35 条が、システム的リスクの緩和のための措置が基本的権利全般に及ぼす影響を考慮するようプロバイダに求めている点である。GDPR 第 5 条及び第 25 条は、データ管理者に、収集される個人データの量、処理の範囲、保存期間、アクセス可能性を考慮し、各特定の目的に必要な範囲でのみパーソナルデータの処理を行うことを義務付けている。

103. DSA 第 35 条(1)(d)は、レコメンダーシステムを含むアルゴリズムシステムの検証・適応策として挙げられており、DSA 第 35 条(1)(e)は、プロバイダが DSA の要件に準拠するため広告システムを適応させ得る旨を規定している。レコメンダーシステムと広告は個人データの処理を伴う可能性があり、特に個人データの収集及び利用慣行に関しては GDPR が適用される（DSA 第 84 項の前文参照）。この問題に関する包括的な分析は、EDPB ガイドライン「ソーシャルメディアユーザーのターゲティング」に記載されており、データ対象者の個人データ管理能力、差別・排除、データ対象者の操作といった複数のリスクを識別している。また「個人データの予期せぬまたは望ましくない利用を伴う可能性があり、これはデータ保護法だけでなく、その他の基本的権利・自由に関する問題も提起する」と指摘している。[138]

104. DSA 第 35 条(1)(i)項で言及される利用者への情報提供措置は、個人データが処理される限りにおいて、GDPR 第 13 条および第 14 条と整合する。プロバイダは、公正かつ透明な処理を確保するために必要な情報がデータ対象者に提供されることを保証すべきである。[139]

105. DSA 第 81 項は、「児童の権利に対するリスクを評価する際、大規模オンラインプラットフォーム及び大規模オンライン検索エンジンのプロバイダは、例えば、未成年者がサービスの設計や機能を理解する容易さ、並びにサービスを通じて未成年者の健康、身体的・精神的・道徳的発達を損なう可能性のあるコンテンツに未成年者が曝される可能性を考慮すべきである」と明確にしている。このようなリスクは、例えば、意図的または非意図的に未成年者の弱さや未熟さを利用したり、依存行動を引き起こす可能性のあるオンラインインターフェースの設計に関連して生じ得る。」さらに、DSA 第 35 条(1)(j)は、プロバイダが「年齢検証やペアレンタルコ

[136] DSA 第 16 条に基づく通知および措置メカニズム、ならびに DSA 第 35 条(1)(c)に基づくコンテンツモデレーションプロセスを含む。

[137] GDPR 第 25 条(1)。

[138] EDPB ガイドライン 8/2020「ソーシャルメディアユーザーのターゲティングに関する指針」、バージョン 2.0、2021 年 4 月 13 日採択、第 4 項。

[139] 規則 2016/679 に基づく透明性に関する第 29 条データ保護作業部会ガイドライン、WP 260 rev.01、2018 年 4 月 11 日。

ントロールを含む、児童の権利を防御するための対象を絞った措置を講じることができる」と述べている。[140]プロバイダが年齢確認を合理的かつ比例的で効果的な緩和と認め、特定されたシステム的リスクに適合させる場合、年齢確認手法は特に、GDPR 第 5 条から第 8 条及び第 25 条の要件、並びに該当する場合は第 22 条の要件を考慮しなければならない。 詳細は、欧州データ保護委員会（EDPB）の年齢確認に関する声明を参照のこと。[141]

106. DSA 第 35 条(1)に列挙された可能な措置は、VLOP および VLOSE のプロバイダ、ならびに DSA 監督当局およびデータ保護監督当局にとって非常に有用であり、GDPR 第 35 条に基づくリスクアセスメントにおいて考慮されるべきである。EBDS は欧州委員会と連携し、システム的リスクの緩和に関するベストプラクティスに関する報告書（DSA 第 35 条(2)）を公表する。また欧州委員会は、DSA 第 35 条(3)に規定されるリスク緩和措置に関する適用ガイドラインを発行できる。

107. 結論として、VLOP および VLOSE のプロバイダは、DSA 第 34 条に基づき、システムリスク（特に、GDPR が二次法で反映する基本権憲章第 8 条に基づく個人データ保護リスクを含む）に関するリスクアセスメントを実施する義務を負う。システムリスクが存在する場合、GDPR 第 35 条に基づく DPIA が義務付けられる可能性が高い。

2.8 行動規範（オンライン広告を含む）（第 45 条、第 46 条及び第 47 条）並びに GDPR 第 40 条に基づく行動規範との関係

108. DSA 第 45 条は、欧州委員会及び監督委員会に対し、DSA の適切な適用に貢献するため、特に「競争及び個人データ保護に関する連合法に準拠しつつ、様々な種類の違法コンテンツ及びシステム的リスクへの対処という固有の課題」を考慮した上で、連合レベルにおける自主的な行動規範の策定を促進・支援することを求めている。

109. 第 45 条(2) DSA は、欧州委員会が「関連する利害関係者」に対し、行動規範の策定への参加を要請することを可能とする。これには、特定のリスク緩和措置を講じることを約束すること、ならびに講じた措置とその結果に関する定期的な報告枠組みを設定することが含まれる。DSA と GDPR におけるリスクアセスメントと緩和措置の相互関係を踏まえ、データ保護当局の適切な関与を確保するとともに、DSA に基づく行動規範と GDPR に基づく行動規範の関係性を明確化することが重要である。この考慮事項は、DSA 第 46 条に基づくオンライン広告向け行動規範の策定において、より一層適用される。

110. 約束事項の達成状況を監視可能とするため、行動規範には測定可能な主要業績評価指標（KPI）を含めるべきである。[142] このような KPI は措置の効果を継続的に測定するために活用でき、EDPB ガイドライン 4/2019「第 25 条 設計時およびデフォルト時のデータ防御」（第 4.6 節、97 項参照）でも提案されている。理想的には、DSA と GDPR の行動規範はこの点において相互補完的であるべきである。

111. DSA 第 46 条では、広告バリューチェーン上のプロバイダが、DSA 第 26 条および第 39 条の要件を超えるさらなる透明性向上に貢献することが推奨されている。これには例えば、GDPR 第 3 章の透明性要件が含まれ得る。

---

[140]本ガイドライン第 2.6 節、第 96 項も参照のこと。

[141]年齢確認に関する EDPB 声明 1/2025（2025 年 2 月 11 日採択）

[142]デジタルサービス法（DSA）第 45 条(3)。

112. この目的は、障害を持つ人々のオンラインサービスへのアクセシビリティ（サービスの適切な設計、情報の容易な発見・理解・利用可能性を含む）を扱う DSA 第 47 条でさらに詳述されている（GDPR 前文 58 項参照）。この主題に関する包括的な議論は、規則 2016/679 に基づく透明性に関する EDPB ガイドラインでも確認できる。[143]

2.9 ガバナンスと執行（ ）

113. 前述のように、DSA に基づいて仲介サービスプロバイダ（VLOP および VLOES を含む）に課せられるいくつかの義務には、仲介サービスプロバイダによるパーソナルデータの処理に影響を与える規定が含まれており、特に GDPR の定義および概念に言及している。EDPB は、憲章第 8 条 (3) 項に従い、GDPR の遵守は独立した機関による管理の対象となることを想起します。[144]

2.9.1 管轄当局間の協力および DPA との誠実な協力の義務

114. DSA は、加盟国が本規則を監督および施行するために 1 つ以上の管轄当局を指定することを規定している。[145] これらの国内管轄当局は、既存の当局である場合もあれば、DSA は、加盟国が電子通信規制当局、メディア規制当局、または消費者保護当局を指定する可能性について明示的に言及している。[146]加盟国が DSA に関連する特定の任務を有する複数の管轄当局を定めている場合、それらの当局は緊密かつ効果的に協力し、各加盟国は国内レベルでの調整を確保するため、そのうちの 1 つを DSC として指定しなければならない。[147] EDPB は、DSA の複数の規定がデータ保護の観点から関連性を持つ一方で、加盟国がこれらの規定の監督及び執行のために、データ保護監督当局以外の国内管轄当局を指定する可能性があることを認めている。

115. DSA は、DSC が相互に、その他の国内管轄当局、欧州デジタルサービス委員会及び欧州委員会と協力することを規定している。ただし、加盟国が、DSC とその他の国内当局との間で、それぞれの任務の遂行に関連する場合に協力メカニズム及び定期的な意見交換を設ける可能性を妨げるものではない。[148]したがって、加盟国が DSA に基づく個人データ保護関連規定の監督・執行を行う管轄当局としてデータ保護監督当局を指定しない場合であっても、DSA は加盟国が国内枠組みのもとで DSC とデータ保護監督当局との間の協力メカニズム及び定期的な意見交換を確立することを妨げるものではない。例えば、データ保護監督機関がデータ保護法に基づき（例：GDPR 第 17 条に基づくデータ対象者の要求に応じなかったデータ管理者に対する個人データ削除命令など）違法コンテンツの特定項目に対する措置命令を発出する場合、DSA 第 9 条の適用が必要となる可能性があるため、このような協力は不可欠である。EDPB は、加盟国がこうし

[143] 2016/679 規則に基づく透明性に関する第 29 条作業部会ガイドライン（WP260 rev.01）、最終改訂・採択日：2018 年 4 月 11 日。

[144] GDPR 第 52 条は、EU 加盟国ごとに指定される監督当局の独立性を確保するための規則を定めており、これは基本権憲章第 8 条(3)および GDPR の前身である指令 95/46/EC 第 28 条(1)に基づく独立性要件に関する欧州司法裁判所(CJEU)の判例法に基づいている。

[145] DSA 第 49 条(1)。

[146] DSA 第 109 項（考慮事項）。

[147] DSA 第 49 条(2)。

[148] DSA 第 49 条(2)。

た状況を考慮し、DSA の対象となる状況において介入が必要となる可能性のある様々な関係者の業務を効率化できる効果的な協力メカニズムを識別するよう奨励している。[149]

116. DSA は、欧州委員会が VLOP および VLOSE プロバイダに対して課される DSA 第 III 章第 5 節に基づく追加的義務の監督・執行に関する排他的権限を有すると規定している。[150] DSA 第 III 章第 5 節に基づく義務以外の VLOP および VLOSE プロバイダに対する監督・執行権限は、欧州委員会と各国の管轄当局が共有する。[151]国家管轄当局は、同一の違反行為について欧州委員会がまだ手続を開始していない場合に限り、VLOP および VLOSE に対する手続を開始できる（[152] ）。これは効率性の観点から、重複を回避し、同一事実に対する二重の訴追禁止の原則（ne bis in idem）の遵守を確保するためである（[153] ）。両者は緊密に連携して DSA を執行することが求められる（[154] ）。

117. DSA は、欧州委員会と DSC 間の任務分担に関する規則を定めており、これにより DSA 下における重複、不整合、および二重処罰の原則に関連するリスクを回避できる。しかし、DSA は、GDPR との規制上の整合性（特に具体的な執行事例の処理において）を確保するための、データ保護監督当局との協議および協力の明示的な義務を規定していない。しかしながら、DSA 第 64 条(3)によれば、「委員会は、本規則に基づく連合全体における体系的・新興課題の評価を支援するため、関連する専門知識を有する他の連合団体・事務所・機関に要請することができる」。さらに、前文第 143 項は、欧州委員会が DSA に定められた義務の効果的な実施及び遵守の監視を支援するため、データ保護当局から独立した外部専門家または監査人を任命する可能性を規定している。EDPB は、これらの規定を歓迎する。これらは、DSA に基づく管轄当局であるか、あるいは関連する専門知識を有するという理由で、委員会とデータ保護監督当局との対話に貢献し、DSA と GDPR の一貫した適用に寄与する可能性があるからである。

118. GDPR も DSA も、DSA に基づく管轄当局とデータ保護監督当局間の協力に関する具体的な規則を定めていない。しかし、基本権憲章第 8 条(3)及び欧州司法裁判所（CJEU）が解釈した EU 基本原則条約（TEU）第 4 条(3)に基づく誠実な協力の原則に照らせば、DSA の執行権限を有する当局（欧州委員会を含む）が要請された場合には、(3) TEU に基づく誠実な協力の原則（欧州司法裁判所による解釈、[155] ）に照らせば、DSA の執行権限を有する当局（欧州委員会を含む）が、その権限の行使において、仲介サービスプロバイダの行為が GDPR の規定（[156] ）に適合しているかどうかを審査するよう求められた場合には、当該国内のデータ保護監督当局または主導的データ保護監督当局と誠実に協議し協力すべきである。逆に、データ保護監督当局が、その権限の行使において、データ管理者またはデータ処理者の行為が DSA の規定に適合しているかどうかを審査するよう求められた場合、DSA の執行権限を有する当局（欧州委員会を含む）と誠実に協議し協力すべきである。異なる枠組みに基づく管轄当局への協議は、とりわけ、

[149]協力メカニズムの例については、2025 年 1 月 16 日に採択された「データ保護と競争法の相互作用に関する EDPB 立場文書」を参照のこと。特に「協力の改善方法」に関する第 4.3 節を参照。

[150]DSA 第 56 条(2)。

[151]DSA 第 56 条(3)。

[152]DSA 第 56 条(4)。

[153]DSA 第 125 項（前文）。

[154]DSA 第 56 条(5)。

[155]欧州司法裁判所判決 2023 年 7 月 4 日 Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537。

[156]これは、データ保護監督当局の専属的権限であるデータ保護法そのものの執行とは異なる。2023 年 7 月 4 日付欧州司法裁判所判決（Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537）44 項及び 45 項参照。

協議を受ける当局が、協議を行う当局によってアセスメント中の仲介プロバイダによる行為（または類似の行為）に関して決定を下した場合に実施されるべきである。

119. このような協力は、データ対象者だけでなく、仲介サービスプロバイダにも利益をもたらす。一方で DSA（デジタルサービス法）、他方で GDPR（一般データ保護規則）がどのように適用されるかについての法的確実性を高めるためである。また、仲介サービスプロバイダの監督に関する規制の不整合に伴う努力の重複や法的リスクを回避することにも寄与する。これは、DSA の執行権限を有する当局（欧州委員会を含む）とデータ保護監督当局による手続や罰則の重複（ ）が、同一事由による二重処罰禁止の原則（non bis in idem）の侵害につながらないことを確保する上でも重要である。[157]

120. DSA を執行する管轄当局から相談を受けたデータ保護監督当局は、合理的な期間内に、当該当局が保有する GDPR の適用に関する疑念を払拭し得る情報を提供して対応すべきである。[158]あるいは、相談を受けたデータ保護監督当局は、GDPR 第 60 条以下（[159] ）に基づき、当該行為が GDPR に適合するか否かの判断を求める決定を得るため、他の関係監督当局または主導監督当局との協力手続を開始する意向がある場合、適切であれば DSA 執行権限を有する当局に通知すべきである。[160]相談を受けた監督当局から合理的な期間内に回答が得られない場合、または当該監督当局が自らの決定を待たずに調査を継続することに異議を唱えない場合、相談した監督当局は調査を継続することができる。[161]

2.9.2 欧州デジタルサービス委員会

121. デジタルサービス法（DSA）に基づく仲介サービスプロバイダの監督に関する助言を行うために設置された欧州デジタルサービス委員会（EBDS）は、欧州委員会が議長を務め、各加盟国のデジタルサービス委員会（DSC）で構成される。[162] 加盟国により DSA に基づく管轄当局として指定されたその他の国内当局（該当する場合、データ保護監督当局を含む）は、国内法で定められている場合に限り、DSC と共に委員会に参加することができる。「議論される事項が当該機関に関連する場合」には、その他の国家機関も招請されることがある。[163]

---

[157]特に欧州司法裁判所は、手続及び処罰の重複が憲章第 50 条に定められた二重処罰禁止原則の本質を尊重しているか否かを分析するにあたり、「どの行為または不作為が手続及び制裁の重複の対象となり得るか、**また異なる当局間の調整が行われることを予測可能とする**明確かつ精密な規則が存在するかどうか**、さらに二つの手続が十分に調整された形で**、かつ近接した時間枠内で**実施されたかどうかを**評価する必要がある」2022 年 3 月 22 日付欧州司法裁判所判決 bpost SA 対 ベルギー競争当局事件（C-117/20、ECLI:EU:C:2022:202）43～58 項参照。

[158]欧州司法裁判所判決（2023 年 7 月 4 日 Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537、57 項及び 58 項）。

[159]GDPR 第 VII 章で規定される協力・整合性メカニズムは、DSA に規定される個人情報保護に関する規定の執行そのものには適用されない。ただし、処理が GDPR の一般規定の対象となる限り、協力・整合性メカニズムは完全に適用される。

[160]欧州司法裁判所判決（2023 年 7 月 4 日）Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537、58 項。

[161]2023 年 7 月 4 日付欧州司法裁判所判決 Meta Platforms 他、C-252/21、ECLI:EU:C:2023:537、59 項。

[162]デジタルサービス法（DSA）第 61 条及び第 62 条。

[163]デジタルサービス法（DSA）第 62 条(1)。

122. さらに、「委員会は*[…]*データ保護などの分野で責任を有する他の連合団体と協力することができる」[164] 。[165] EDPB は、DSA と GDPR の適用における規制間の整合性を確保するため、EBDS と EDPB 間の協力が重要であると考えている。実際、EBDS の任務には、DSA の執行権限を有する当局が VLOP または VLOSE（デジタルサービスが個人データ保護という基本的権利に及ぼす悪影響を分析するリスクアセスメントなど）の監査報告書および結果を分析する際の支援（[166] ）、DSA で規定されているように、関連する利害関係者との協力による欧州標準、ガイドライン、報告書、テンプレート、行動規範の開発および実施の支援と促進が含まれる。さらに、DSA の対象事項に関する新たな課題の特定を支援するものとする。[167]

[164]DSA 第 62 条(5)。

[165]DSA 第 134 項（前文）。

[166]DSA 第 34 条(1)(b)

[167]DSA 第 63 条(1)(e)