

Data Protection Legal Update

個人情報保護・データプライバシーニュースレター

2025 年 12 月 No.62

GDPR の改正提案を含む欧州委員会による Digital Omnibus の公表

弁護士 森 大樹

弁護士 早川 健

はじめに

欧州では、GDPR（General Data Protection Regulation: 一般データ保護規則）や AI 法（Artificial Intelligence Act）をはじめとしてデジタル領域における広範な立法を通じたルール作りが進められてきていますが、その一方で、規制が複雑であることによる欧州におけるビジネスの競争力への悪影響の懸念もあり、このため、規制の目的を損なうことなく事業者のコンプライアンスを促進するための規制の適用の最適化が課題となっています。

このような状況下で、2025 年 11 月 19 日、欧州委員会により、デジタルに関する様々な法令について規則遵守のコスト削減、規制の目標を達成する確実性の向上、企業にとって競争優位性につながることを目的とした Digital Omnibus の提案が公表されました¹。

Digital Omnibus²は、GDPR のみならずその他の法令の改正提案を含んでおり、Digital Omnibus の一部として別途 AI 法の改正提案もなされています³が、以下では、2018 年 5 月の適用開始以来、実務上の対応が浸透してきた GDPR についての改正提案の内容を主に紹介します。

Digital Omnibus における主な GDPR の改正提案の内容

1. 「個人データ」該当性についてエンティティ毎に判断すべきこと（3 条 1 項(a)）

[現行の規定]

GDPR4 条(1)では「個人データ」の定義を「識別された自然人又は識別可能な自然人（「データ主体」）に関する情報を意味する。識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す一つ又は複数の要素を参照することによって、直接的又は間接的に、識別される者をいう。」と規定しています。

[改正提案]

Digital Omnibus では、「個人データ」の該当性について、情報を処理するエンティティにおいて利用可能な手段を考慮して該当性を判断すべきことの明確化、すなわち、個人データの当該定義の後に、あるエンティティが、ある情報について、合理的に用いる手段を考慮して当該情報に関連する自然人を識別することが

¹ https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718

² <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>

³ <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal>

できない場合、たとえ潜在的なその後の取得者が自然人を識別することができる方法を有しているとしても当該情報は当該エンティティにとって個人データとみなされない旨を追加することが提案されています。

当該提案は、「個人データ」の定義の自然人の識別性そのものについての判断基準を変更するわけではないと考えられるものの、近時の欧州司法裁判所による仮名化の処理に係る個人データの該当性についてエンティティ毎に判断する旨を判示した判決⁴を念頭に置いており、情報を処理するエンティティにおいて自身にとって利用可能な手段によって個人データの該当性を判断すべきという点は、情報を複数エンティティ間で共有する際の個人データの該当性に係る判断の明確化にもつながりうると考えられます⁵。

2. 特別な種類のデータの処理に係る GDPR9 条の例外要件 (AI システム・モデル⁶及び生体データについて) (3 条 3 項)

[現行の規定]

GDPR9 条 1 項は、「人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの処理、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの処理は、禁止される」と定め、同項で掲げる特別な種類の個人データの処理については、同条 2 項各号で定めるデータ主体の明確な同意がある場合等の限定的な場合に限り認めています。

[改正提案]

Digital Omnibus では、このような特別な種類のデータの処理が許される場合について、二つの規定を追加することを提案しています。

- (1) AI システム又は AI モデルの開発及び運用のために特別な種類の個人データを処理する場合であって、特別な種類の個人データの収集やその他の処理をしないことについての適切な組織的及び技術的措置がとられているとき（ただし、この場合でも、管理者は、使用されるデータセットや AI システム・AI モデルに特別な種類の個人データが含まれることが判明したときの削除義務や、削除に過大な負担を要する場合に第三者へ利用可能にならないように効果的に保護する義務を負います。）
- (2) 自然人を一意に識別することを目的とする生体データの処理について、データ主体の身元を確認するために必要であり、かつその確認のためのデータと手段がそのデータ主体のみの管理下にある場合

(1)については、AI システムや AI モデルの開発・運用においては個人データを収集・利用する場合に特別な種類の個人データが含まれうることを念頭に、一定の対策をとることによって AI システムや AI モデルの開発・運用が GDPR に抵触しないことを明確化するという点で実務上の対応に配慮しようとする趣旨と考えられます。もっとも、どのような措置をとれば適切な組織的及び技術的措置といえるかについては必ずしも明確ではなく、また、使用されるデータセットや AI システム・AI モデルに特別な種類の個人データが含まれることが判明した場合の対応に係る義務が実務上遵守可能なものであるのかといった点が課題になりうると考えられます。(2)については、本人認証目的で生体データを利用することへの実務上の対応に配慮しようとする趣旨と考えられます。

⁴ CJEU, Case C-413/23P (SRB v. EDPS), 2025 年 9 月 4 日

<https://curia.europa.eu/juris/document/document.jsf?jsessionid=16C018E9F2893C3E0C4A571DB193AF08?text=&docid=303863&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11181678>

⁵ なお、仮名化に関しては、Digital Omnibus において、欧州委員会が、欧州データ保護会議と共に、仮名化された情報があるエンティティにとって個人データを構成しないかどうかについての方法及び基準を特定することも提案しています（3 条 10 項）。

⁶ Digital Omnibus では、AI システム及び AI モデルについて、GDPR9 条の特別な種類の個人データに係る規律以外にも、GDPR88c 条として、個人データの処理につき GDPR6 条 1 項(f)の正当な利益に依拠しうる旨の条項の加筆も提案しています。

3. データ主体の権利行使が「明らかに根拠のない/過剰」である場合の明確化（3条4項）

[現行の規定]

GDPR12条5項は、GDPRに基づくデータ主体の権利行使については、無償で行うことができることを定めつつ、明らかに根拠のない場合又は過剰な性質のものである場合には、合理的な手数料を徴収すること及び要求された行為を拒むことができると定めています。

[改正提案]

Digital Omnibus では、上記の「明らかに根拠のない場合又は過剰な性質のものである場合」として、アクセス権の行使について自身のデータの保護以外の目的で濫用している場合を追加する旨を提案しています。

当該提案は、データ主体の権利行使に対応する事業者の負担に配慮したものと考えられます。

4. 本人への情報提供義務の例外（3条5項）

[現行の規定]

GDPR13条1項から3項では、データ主体から個人データを直接取得する場合の管理者の身元・連絡先、予定している個人データの処理の目的等の情報提供義務を規定しているところ、同条4項は、同条1項から3項の義務について、データ主体が既にその情報を有している場合にはその範囲で適用されないと規定しています。

[改正提案]

Digital Omnibus では、GDPR13条4項を改正し、管理者による収集がデータ主体と管理者との間の明確で限定された関係で行われ、かつ、管理者がデータ集約的な活動を行っていない場合であって、データ主体が同条1項(a)から(c)の情報を既に有していると合理的に推測できる状況では情報提供義務を適用除外とすること、ただし、管理者がデータを他の取得者に送信する場合、データを第三国に移転する場合、自動化された意思決定を行う場合、又はその処理がデータ主体の権利に高いリスクをもたらす可能性がある場合については適用除外に含まないとする⁷を提案しています。

当該提案は、GDPR13条4項の適用除外の場面について、データ主体の権利利益と管理者の負担とのバランスに配慮しようとしているものと考えられます。

5. プロファイリングを含む個人に対する自動化された意思決定に係る要件の明確化（3条7項）

[現行の規定]

GDPR22条は、1項で、データ主体が、当該データ主体に関する法的効果を発生させる、又は、当該データ主体に対して同様の重大な影響を及ぼすプロファイリングを含むもっぱら自動化された処理に基づいた決定の対象とされない権利を有すると規定し、2項で、当該権利の対象とならない場合として、①データ主体とデータの管理者の間の契約の締結又はその履行のために必要となる場合（同項(a)）、②EU法又は加盟国の国内法によって認められる場合（同項(b)）及び③データ主体の明示的な同意に基づく場合（同項(c)）を掲げています。

[改正提案]

Digital Omnibus では、GDPR22条に基づく個人に対する自動化された意思決定が上記①から③の場合にのみ行うことができる旨の規定を維持しつつ、上記①のデータ主体とデータの管理者の間の契約の締結又はその履行のために必要となる場合について、その「必要性」の要件が、意思決定が完全に自動化された手段以外の方法で行われるかどうかにかかわらず適用される旨の規定を提案しています。

⁷ この他にも、Digital Omnibus では、学術研究目的での処理の場合の例外規定も提案されています（3条6項）。

当該提案は、GDPR22 条について現行の規定がデータ主体の権利の建て付けになっているのに対して、データの管理者/処理者における処理が許容される場合としての性質を明確化すると共に、自動化された手段以外で個人に対する意思決定を行うことができる場合であっても上記①に依拠できることを明確化しようとしていると考えられます。

6. データ侵害時の報告義務の緩和（3 条 8 項）

[現行の規定]（下線は筆者による。以下同じ。）

GDPR33 条 1 項では、監督機関に対する個人データ侵害の通知について、「管理者は、その個人データ侵害が自然人の権利及び自由に対するリスクを発生させるおそれがない場合を除き、不当な遅滞なく、かつ、それが実施可能なときは、その侵害に気づいた時から遅くとも 72 時間以内に、55 条に従って所轄監督機関に対し、その個人データ侵害を通知しなければならない。」と規定しています。なお、GDPR34 条 1 項では、データ主体に対する個人データ侵害の連絡について、「個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合」の不当な遅滞なき連絡を規定しています。

[改正提案]

Digital Omnibus では、GDPR33 条に基づきデータの管理者が所轄監督機関に対してデータ侵害を通知する義務について、以下の修正を提案しています。

- (1) データ侵害がデータ主体の権利及び自由に対する高いリスクを発生させる可能性がある場合に監督機関への通知が必要とされること
- (2) 当該通知にあたり、通知の期限を 96 時間に延長し、NIS2 指令⁸に従い設置された単一窓口（single-entry point）を通じて通知すること
- (3) 欧州データ保護会議は、データ侵害通知の共通テンプレート案を作成し、欧州委員会に提出する義務があること

当該提案は、(1)について監督機関に対する個人データ侵害の通知義務が生じる場合を、データ主体に対するデータ侵害の連絡義務が生じる場合と一致させること、また、(2)及び(3)については手続きをシンプルにすることを意図しているといえ、データ侵害が発生した場合の実務上の対応に影響のある提案内容となっています⁹。

7. データ保護影響評価が必要な場合の EU レベルでの共通化（3 条 9 項）

[現行の規定]

GDPR35 条 1 項は、データ保護影響評価について、「処理の性質、範囲、過程及び目的を考慮に入れた上で、特に新たな技術を用いるような種類の処理が、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合、管理者は、その処理の開始前に、予定している取扱業務の個人データの保護に対する影響についての評価を行わなければならない」と規定し、また、同条 4 項及び 5 項は、加盟国の監督機関について、当該義務の対象となるべき処理業務の種類のリストを作成・公表すべきこと、及び当該義務の対象とならない処理業務の種類のリストを作成・公表できることを規定しています。

[改正提案]

Digital Omnibus では、欧州データ保護会議が、上記の加盟国の監督機関が作成すべき/作成することができ

⁸ Directive (EU) 2022/2555

<https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

⁹ また、Digital Omnibus では、Network and Information Security II Directive (NIS2 指令)、Digital Operational Resilience Act、eIDAS Regulation 及び Critical Entities Resilience Directive に基づく報告も一元化することが提案されています。

るとされていたデータ保護影響評価を必要とする処理業務及びデータ保護影響評価を必要としない処理業務のリストを準備すべきこと、また、データ保護影響評価を実施するための共通テンプレート及び共通手法を準備すべきこと、を提案しています。

当該提案によって、これまで加盟国の監督機関毎に作成されていたリストが、欧州データ保護会議により準備されることにより、データ保護影響評価の実施の要否やその実施手法が EU レベルでより明確になることが期待されます。

8. Cookie に係る規定の追加（3 条 15 項）

[現行の規定]

上記 1.のとおり、GDPR4 条(1)では「個人データ」の定義として、自然人を識別するオンライン識別子についてその定義に含むものの、Cookie については ePrivacy 指令においてより具体的な規律がなされています。

[改正提案]

Digital Omnibus は、88a 条を GDPR に新設し、GDPR 上の規律として、Cookie に関して、自然人の端末機器上での個人データの保存又は保存されている個人データへのアクセスに対して原則としてデータ主体の同意を取得する必要があることを定めると共に¹⁰、その同意に関して、以下の要件を定めることを提案しています。

- (1) データ主体がボタンのワンクリック又は同等の手段で簡単かつ分かりやすい方法で同意の要求を拒否できるようにすること
- (2) データ主体が同意した場合、管理者はデータ主体の同意に適法に依拠できる期間中、同じ目的のために新たな同意の要求を行ってはならないこと
- (3) データ主体が同意の要求を拒否した場合、管理者は少なくとも 6 か月間、同じ目的のために新たな同意の要求を行ってはならないこと

また、Digital Omnibus は、併せて、88b 条を新設し、データ主体が自動かつ機械によって読み取り可能な方法で、同意を与えること、同意の要求を拒むこと及び GDPR21 条 2 項の異議を述べる権利の行使をできるようなオンラインインターフェースを管理者が確保することも提案しています。これらの同意に係る規律は、データ主体における Cookie に関しての同意疲れにも配慮し、Cookie バナーの使用の削減・簡素化を意図しているものと考えられます。

Digital Omnibus におけるその他の改正提案の内容（AI 法）¹¹

Digital Omnibus においては、上記の GDPR に係る改正提案の他にも、例えば、AI 法について、①ハイリスク AI についてのルール適用のタイムラインを見直すこと¹²、②簡素化した技術文書の要件を含む中小企業（small and medium-sized enterprises: SMEs）向けの簡素化の規定の適用対象について、中規模の事業者（small mid-cap enterprises: SMCs）にも拡大すること、③AI オフィスも特定の AI システムについて EU

¹⁰ Digital Omnibus では、同意に依拠しなくてよい例外的な場合として、①電子通信ネットワークを介した電子通信の送信を行う場合、②データ主体が明示的に要求したサービスを提供する場合、③オンラインサービスの利用状況に関する集約情報を作成し、そのサービスの視聴者を測定する場合（ただし、オンラインサービスの管理者が自己使用のためのみに行う場合に限り）、④データ主体が要求したサービスやそのサービスの提供に使用される端末機器のセキュリティを維持又は回復する場合、を提案しています。

¹¹ この他にも、Digital Omnibus では、Data Act についての提案もされています。

¹² 具体的には、①AI 法 6 条 2 項及び ANNEX III のハイリスク AI システムについては、欧州委員会が遵守を支援するための適切な措置が利用可能であることを確認する決定を採択した後 6 か月、又は遅くとも 2027 年 12 月 2 日、また、②AI 法 6 条 1 項及び ANNEX I のハイリスク AI システムについては、欧州委員会が遵守を支援するための適切な措置が利用可能であることを確認する決定を採択した後 12 か月、又は遅くとも 2028 年 8 月 2 日、と提案しています。また、2026 年 8 月 2 日までに市場に置かれた汎用目的 AI システムについては 2027 年 2 月 2 日までに AI 法 50 条 2 項を遵守する措置を講じるべき旨の条項の加筆も提案されています。

レベルでの規制のサンドボックスを創設できるようにし、また実環境テストを利用できる AI システムを拡大すること、④AI オフィスの権限を強化し汎用目的 AI モデルの AI システムの監督を集権化すること等も提案しています。

今後に向けて

今回公表された Digital Omnibus は、欧州委員会による提案の位置付けであり、法律として成立するためには、EU 理事会・欧州議会・欧州委員会の各代表による「三者対話 (trilogue)」を経るなどして EU 理事会と欧州議会による共同採択を経る必要があるため、その内容は今後の手続の中で大きく変わる可能性があります。

もっとも、今回公表された Digital Omnibus の他にもデジタル規制については改正提案がなされていくことも見込まれるため、日本企業においても今回の提案内容を含めて状況を注視していく必要があり、当事務所としても、引き続き、日本企業の皆さまのご参考になる情報発信をして参りたいと考えております。

2025 年 12 月 2 日

[執筆者]



森 大樹（弁護士・パートナー）

oki.mori@nagashima.com

2001 年慶應義塾大学法学部法律学科卒業、2002 年弁護士登録、長島・大野・常松法律事務所入所。2007 年～2009 年内閣府・内閣官房・消費者庁にて勤務。訴訟・紛争解決業務に加えて、国内外の個人情報・プライバシー関係、消費者関連法（景品表示法、製品事故・リコール、PL 法、消費者契約法など）を中心として、企業法務全般に従事している。別冊 NBL No.162「日米欧 個人情報保護・データプロテクションの国際実務」（編集代表）など個人情報保護法・GDPR に関する著作も多数ある。



早川 健（弁護士・カウンセラー）

takeshi.hayakawa@nagashima.com

2006 年東京大学法学部卒業。2009 年早稲田大学大学院法務研究科修了。2010 年長島・大野・常松法律事務所入所。2016 年 Duke University School of Law 卒業 (LL.M.)。2017-2018 年ヤフー株式会社（現 LINE ヤフー株式会社）勤務。2018-2020 年個人情報保護委員会勤務。個人情報保護、危機管理・コンプライアンスの案件を中心にリーガルサービスを提供している。個人情報保護委員会事務局での在任中は、欧州、米国、アジアなど世界の個人データ保護法令の動向についての情報収集等を担当。

[編集者]

鈴木 明美（弁護士・パートナー） akemi.suzuki@nagashima.com

森 大樹（弁護士・パートナー） oki.mori@nagashima.com

水越 政輝（弁護士・パートナー） masaki.mizukoshi@nagashima.com

本ニュースレターは、各位のご参考のために一般的な情報を簡潔に提供することを目的としたものであり、当事務所の法的アドバイスを構成するものではありません。また見解に亘る部分は執筆者の個人的見解であり当事務所の見解ではありません。一般的情報としての性質上、法令の条文や出典の引用を意図的に省略している場合があります。個別具体的事案に係る問題については、必ず弁護士にご相談ください。

ニュースレターの配信登録を希望される場合には、<<https://www.nagashima.com/newsletters/>>より「Legal Lounge」に会員登録ください。

ニュースレターに関するお問い合わせ等につきましては、<newsletter@nagashima.com>までご連絡ください。
