FAQ

データ法

2024 年 9 月 13 日

バージョン 1.1

データ法（規則(EU)2023/2584）は、データ生成技術に投資する人々の利益を守りつつ、データから生成される価値の市場関係者間での公平な配分を確保するために、調和された水平ルールを確立するものである。

データ法の序文については、「データ法の説明」のファクトページを参照されたい。

この「よくある質問と回答（FAQ）」は、データ法施行の約 1 年前に公表されたものであり、関係者が法規定を実施する際の一助となることを目的としている。この FAQ は、広範な利害関係者との対話の成果であり、必要に応じて更新される「生きた文書」であることを意図している。バージョン履歴はこの文書の最後にある。

この文書は、欧州委員会の公式見解を代表するものとみなされるべきではない。FAQ への回答は、適用される法律から派生する権利と義務をいかなる形でも拡張するものではなく、また、いかなる追加要件も導入するものではない。表明された見解は権威あるものではなく、欧州連合司法裁判所での立場を含め、欧州委員会が将来取る可能性のある行動を予言するものではない。

ここに記載されていないご質問がある場合は、当社までご連絡いただければ、可能な限り迅速に対応させていただく。データ法の実施に関する苦情については、加盟国のデータコーディネーターに連絡することを検討されたい。

欧州連合、2024 年

欧州委員会文書の再利用方針は、欧州委員会文書の再利用に関する 2011 年 12 月 12 日付委員会決定 2011/833/EU（OJ L 330, 14.12.2011, p.39）によって実施されている。特に断りのない限り、本文書の再利用はクリエイティブ・コモンズ 表示 4.0 国際（CC BY 4.0）ライセンス（https://creativecommons.org/licenses/by/4.0/）の下で許可されている。つまり、適切なクレジットを付与し、変更箇所を明記すれば再利用が許可される。

内容

他の EU 法との相互作用 4

IoT におけるデータへのアクセスと利用 6

ユーザーに関するセクション..... 11

データホルダーに関するセクション 15

サードパーティに関するセクション 23

公正、合理的かつ非差別的（FRAND）な条件、補償、紛争解決..... 24

企業間データ共有契約における不公正 25

企業対政府のデータアクセス..... 27

データ処理サービスを切り替える 30

第三国当局による EU 域内で保有される非個人データへの違法なアクセスと移転..... 33

相互運用性 35

施行 36

次のステップと将来の行動 38

データ法 FAQ バージョン履歴..... 39

他の EU 法との相互作用

1)　データ法は一般データ保護規則とどのような関係にあるか？

一般データ保護規則（GDPR）は、データ法に基づくすべての個人データ処理活動に全面的に適用される。データ法は個人データの保護を規制するものではない。その代わりにデータ法は、EU のデータ経済圏におけるデータへのアクセスと使用に関連する明確なルールを確立することによって、データ共有を強化し、データの価値の公正な分配を可能にしている。

場合によっては、データ法は GDPR を規定し補完している（例：IoT 対象からのデータのリアルタイム・ポータビリティ）。また、データ法がサードパーティによるデータの再利用を制限している場合もある（データ法第 6 条など）。GDPR とデータ法が矛盾する場合、個人データ保護に関する GDPR の規則が優先する（データ法第 1 条 5 項参照）。

2)　データ法と GDPR の関係は、個人データの執行と保護にどのような影響を与えるか？

データ法は、個人データ保護に関する規則を執行するデータ保護当局（DPA）の権限を尊重している。データ法は、DPA と他の管轄当局との間の首尾一貫した執行・協力メカニズムを提供している。

データ法第 1 条 5 項は、GDPR がデータ法の枠組みにおけるパーソナルデータの処理に適用されることを定めている。この文脈では、DPA が GDPR に直接由来する義務を執行する権限を有することを想起させる。

第 37 条 3 項は、個人データの保護に関する限り、DPA はデータ法の適用を監視する責任を負い、GDPR に規定された任務と権限に依拠できると規定している。このことは 107 項にも記載されている。例えば、(i)データ対象者であるユーザーが要求するすべての個人データを受け取ったか、またはポートを許可されたか、(ii)データ保有者がどのデータを個人データとみなすべきかを正しく認定したか、(iii)データ対象者でないユーザーが個人データを要求し、ポートをするために GDPR 上の有効な法的根拠が存在するか、などをアセスメントする権限である。第 37 条 3 項はまた、アクセス権およびポーティング権がデータ法と GDPR の両方に適用される場合、またはデータ法の適用における個人データ保護に関連するその他の不満がある場合、データ対象者が 2 つの異なる認可機関に行く必要がないことを保証する。

より一般的には、欧州委員会は、欧州データ保護監察機関（EDPS）と欧州データ保護委員会（EDPB）が欧州データ革新委員会（European Data Innovation Board）に加盟することを含め、EU でデータ法を施行する当局間の強固な協力関係の促進に努めている。

3)　データ法は、他の EU 法に基づく既存のデータ共有義務とどのように相互作用するか？

データ法は、経済の全分野にわたってデータへの公正なアクセスと利用を大幅に強化することを目的とした水平的な法律である。特に第 III 章は、データ保有者が EU 法または国内法に基づいてデータ取得者とデータを共有する義務を負う場合の条件、補償、技術的保護措置に関する枠組みを定めている。

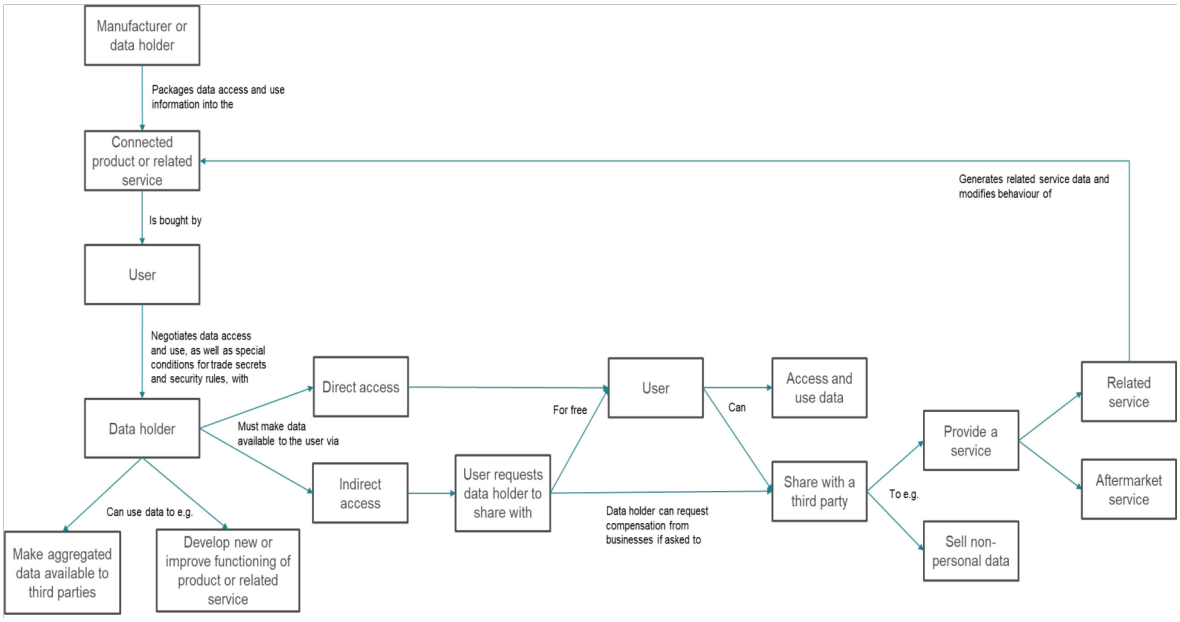
より具体的には、第 44 条はデータ法と、データへのアクセスと利用に関する規則を含む他の EU 法との相互作用を構成する 2 つの重要な側面、すなわち発効時期（第 44 条 1 項）と分野別の特殊性（第 44 条 2 項）を取り上げている。

第 44 条 1 項によれば、2024 年 1 月 11 日（データ法の発効）以前に発効したデータ共有義務は影響を受けない。EU の法律が 2024 年 1 月 11 日から 2025 年 9 月 12 日（データ法の発効）までの間にデータに関する規則を導入する場合、整合性を確保するために最善の努力を払うべきであるが、その法的義務はない。

データ法はデータへのアクセス、共有、使用に関する水平的な規則を定めている。しかし、第 44 条 2 項は、必要な場合には、実務的・技術的様式（安全性、標準化、技術的事項など）や、データ保有者のアクセス権や行為に関する具体的な制限を定めた分野別法によってデータ法を補完することを認めている。しかし、このような分野別規則の作成は、不必要な複雑さを避けるため、可能な限り データ法に定められた原則に合致するよう慎重に行うべきである。データ法の原則は、そのような分野別規則で特に規定されていない「データへのアクセス」 に関するすべての事項に適用される。

「IoT」の文脈におけるデータへのアクセスと利用

第 *II* 章の実践例



4) どのデータが対象なのか？

データ法第 3 条、第 4 条、第 5 条に規定されているデータアクセス権の対象となるデータは、いくつかの 要因によって決定される。一般的に言えば、製造事業者の技術的設計の結果としてデータ保有者が容易に入手できる生データおよび前処理済みデータ（簡単に言えば「生データだが使用可能な」データ）は、第Ⅱ章で規定される強制的なデータ共有義務の対象者である。

IoT データへのアクセスと利用 - データ法第 2 章

ファクター	説明	法文での言及
製品データ	接続された製品によって取得、生成、または収集されるデータであって、その性能、使用、 または環境に関連するもの。コネクテッド・プロダクトに付随する（例えば取扱説明書や包装に記載された）純粋に記述的なデータは、製品データではない。接続された製品「に関する」情報が関連する唯一の状況は、第 3 条に基づく契約前の透明性義務である。	リサイタル 15、第 2 条 (15)
関連サービスデータ	関連サービスの提供中に、接続された製品に関連するユーザーの行動、不作為、およびイベントを表すデータ。	リサイタル 15 と 17、第 2 条 (16)

入手しやすいデータ	製品データおよび関連サービスデータであって、データ保有者が簡単な操作を超えて不相応な労力をかけることなく入手できるもの。容易に入手可能なデータ」の定義には、生成または収集の時期に関する言及は含まれていない。データ法の適用開始後に生成・収集されたデータのみが、第 II 章の適用範囲に含まれる。	リサイタル 20 と 21、第 2 条(17)
データの充実度	対象範囲：生データおよび前処理済みデータで、理解しやすく利用しやすくするために必要なメタデータを伴うもの。例えば、物理的な量や質、あるいは物理的な量（温度、圧力、流量、音声、pH 値、液面、位置、加速度、速度など）の変化を判断することで、収集したデータをより広いユースケースで理解できるようにする目的で、単一のセンサーまたは接続されたセンサー群から収集したデータ。 対象外：高度にエンリッチされたデータ、すなわち推論または派生されたデータ、あるいは追加投資（独自の複雑なアルゴリズムによるものを含む）の結果得られるデータを意味する。さらに、知的財産権の対象となることが多いコンテンツ（テキスト、オーディオ、オーディオビジュアルコンテンツなど）。	リサイタル 15
個人データと非個人データ	利用者は、個人データであるか否かを問わず、接続された製品または関連サービスによって生成されたすべてのデータにアクセスする権利を有する。 しかし、個人データ処理は GDPR の規則によって管理されるため、データ法で規定されたユーザーの権利は GDPR に準拠して行使されなければならない。データ対象者でもデータ保有者でもないユーザーは、パーソナルデータの処理について GDPR 第 6 条に基づく有効な法的根拠を持たなければならない。質問 26 では、非個人データへのアクセス、使用、共有についてさらに詳しく検討する。	リサイタル 25 と 35
営業秘密	データ法は、営業秘密の保護に関連する法的防御を修正するものではない。例えば、2016 年の営業秘密指令は引き続き適用される。データ法は営業秘密を保護するための新たな仕組みを設ける。この仕組みは「営業秘密ハンドブレーキ」として知られ、第 20 問でさらに検討される。	リサイタル 31、第 4 条(6)、第 5 条(9)

5)　「コネクテッド製品」とは何か？

コネクテッド製品とは、その使用、性能、環境に関するデータを生成、取得、収集することができ、このデータを有線または無線接続を介して通信できる製品を指す。これには、アドホック・ベース（保守作業中など）での製品外とのデータ・コミュニケーションも含まれる。コネクテッド製品は、経済社会のあらゆる分野で見られる。スマート家電、家電製品、産業機械、医療機器、スマートフォン、テレビなどである（参考資料 14）。

主にデータの保存、処理、送信の機能を果たす製品（サーバーやルーターなど）は、ユーザーが所有、レンタル、リースしている場合を除き、第 II 章のデータ共有義務対象外である。

同様に、コネクテッド製品（ワゴン車、飛行機、車両など）が機能するために特定のインフラ（鉄道、空港、高速道路など）を使用しなければならないという事実は、そのコネクテッド製品のユーザーが、例えばそのインフラの一部であるセンサーによって生成的なデータにアクセスする権利を与えるものではない。アクセスが認められるのは、ユーザーがインフラに組み込まれたセンサーの所有権または契約上の権利を得た場合のみである。最後に、データ法は、プロトタイプは製造段階が完了していないため、対象外であると規定している。

6)　コネクテッド・プロダクトがデータ法の適用範囲に入るかどうかは何で決まるか？

接続された製品が「連合市場に上市」された場合、データ法の適用範囲に入る（第 2 条 22 項）。上市」とは、製造事業者間の所有権、占有権、その他の財産権の移転のことであり、製造段階以降に発生する。接続された製品が「上市」されるのは一度だけである。それ以降の操作はすべて「市場で入手可能」とみなされる（第 2 条 21 項）。上市という概念は、製品の種類ではなく、個々の製品を指す。したがって、データ法に規定された要件は、EU 市場に上市された個々の製品にのみ適用され、その種類の製品すべてに適用されるわけではない。

欧州委員会の通知「EU 製品規則の実施に関する "ブルーガイド"」（2022 年）は、データ法の製品に関する規則のインスピレーションとなり、このトピックに関する包括的なガイダンスを提供している。例えば、ブルーガイドでは、製品が「上市」されたとみなされない状況を特定している。これには、(i)第三国の消費者が第三国に滞在中に製品を購入し、その消費者が個人使用のために EU 域内に持ち込む場合、(ii)製品が第三国への輸出を目的として加盟国で製造される場合などが含まれる。

7)　EU 市場に上市されたコネクテッド製品が、海外で使用される際にデータを生成した場合はどうなるか？

コネクテッド・プロダクトが EU 域内で上市され、その後 EU 域外で使用される場合、そのコネクテッド・プロダクトによって EU 域内外で生成されたデータは、データ法に従ってユーザーに入手可能とされるべきである。

質問 6 への回答で説明したように、コネクテッド・プロダクトが EU 域内で上市された場合、データ法の適用範囲に入る。つまり、「移動可能な」コネクテッド・プロダクト（例えば、船舶、航空機、列

車、自動車）は、他のコネクテッド・プロダクトと同様に扱われるべきである。船舶、飛行機、列車、自動車が EU 領土内または EU 水域内を流通するだけでは、所有権の移転がないため、コネクテッド・プロダクトが「EU 上市」されたとみなすには不十分である。

データ法の規則は、個人または事業体と対象物との間の所有権および賃貸借に関する民法上の関係を基礎としている。自動車、鉄道車両、飛行機などのコネクテッド・プロダクトが加盟国で登録されているという事実は、当該コネクテッド・プロダクトが EU 上市されたことを示す指標となる。

8) 「関連サービス」とは何か？

関連サービスとは、コネクテッド製品の動作にリンクさせることができ、例えばデータやコマンドをコネクテッド製品に送信することによって、このコネクテッド製品の機能に影響を与えるデジタルサービスである（例えば、照明の明るさを調整するアプリや、冷蔵庫の温度を調節するアプリ）。

デジタルサービスが関連サービスとみなされるためには、基本的に 2 つの条件が満たされなければならない：

- 接続された製品とサービスプロバイダーとの間で、双方向／双方向のデータ交換が行われなければならない。
- サービスは、接続された製品の機能、動作、または操作に影響を与えなければならない。

コネクテッド・プロダクトの「機能」を決定することは、現在進行形で進化している課題である。デジタルサービスが関連サービスであるかどうかをさらに明確にするためには、実務と裁判所の解釈が不可欠な役割を果たすだろう。デジタルサービスが関連サービスかどうかをさらに絞り込むには、以下の要素が有用であろう：

- その製品カテゴリーに対するユーザーの期待である；
- コネクテッド製品および/またはデジタルサービスに付随するマーケティング；
- 契約交渉である；
- デジタルサービスの代替可能性である；
- 接続された製品にデジタルサービスをプリインストールする。

すべてのデジタルサービスではないが、ほとんどのデジタルサービスが関連サービスのカテゴリーに入る。以下のデジタルサービスは関連サービスとはみなされない：接続、電力供給、アフターマーケット・サービス（補助的なコンサルティング、分析、金融サービス、定期的な修理・保守など）（レシタル 17 参照）。

関連サービスを提供するためには、プロバイダはまず製品データを受け取らなければならない。ユーザーとプロバイダとの間に契約関係が成立し、データ作成につながる関連サービスが提供されると、プロバイダはデータ保有者となる。

9)　コネクテッド製品が転売された場合（「中古コネクテッド製品」）はどうなるか？

コネクテッド・プロダクトの使用によって生成的なデータにアクセスするユーザーの権利に関して言えば、データ法は、コネクテッド・プロダクトの「ファーストハンド」と「セカンドハンド」を区別していない。

接続された製品が（再）販売される場合、販売者は第 3 条に概説されている「透明性義務」を遵守しなければならない。これにより、販売者は将来の所有者がデータ法に基づく新たなデータアクセス権を行使するために必要な情報を提供する必要がある。その結果、将来の所有者は、データ所有者が誰であるかに加え、生成的データへのアクセスと使用の方法についても知らされることになる。この FAQ の他のセクションは、データ保有者が正当な利用者をどのように特定できるかなど、関連する問題を扱っている。

10）データ法第 2 章に基づく義務は、適合性評価や型式承認の仕組みとどのように関係するか？

データ法は、特定の型式承認や適合性評価制度の対象者（自動車、航空機、医療機器など）を含む、すべてのコネクテッド製品に適用される。

データ法には適合性評価の仕組みに関する具体的な規定はないが、データ法の義務は適用される。したがって、一般規定として、コネクテッド・プロダクトは、適用されるすべてのデータ法規定に準拠し、適用される法律に従って適合性評価が実施された場合にのみ、上市することができる。言い換えれば、コネクテッド・プロダクトが適合性評価手続きを受ける具体的な必要性は、データ法以外の法律で定められた要件によって決定される。

ユーザーに関するセクション

11) 「ユーザー」とは何か？

第 2 条(12)の一般原則は、「ユーザー」とは、接続製品を所有するか、その接続製品を使用する一時的な権利が契約上譲渡された自然人または法人、あるいは関連するサービスを受ける自然人または法人である。

このことは、ユーザが接続された製品に関して安定した権利（所有権、賃貸契約やリース契約による権利など）を有していることを意味する。このようなユーザーは、データ法に基づき、接続製品によって生成されるデータに対して法的権利を有する。

12) データ法は EU 域外に設立されたユーザーにも適用されるか？

第 1 条(3)(b)によれば、利用者は EU 域内に設立されていなければならない。利用者は、データが EU 域内に保存されているか域外に保存されているかにかかわらず、データ法に基づいてデータへのアクセスを要求することができる。

13) ひとつの接続製品に複数のユーザーを存在させることは可能か？また、そのアクセスはどのようにガバナンスされるべきか？

様々な行為者が、コネクテッド・プロダクトの使用に関連する契約上の取り決めに基づく法的権利を有する可能性がある。したがって、複数の人が同一のコネクテッド・プロダクトのユーザーとなることは十分に可能である。このような場合、データ保有者は、各ユーザが権利を有するデータにアクセスできることを保証するための仕組みを備えるべきである。また、ユーザーは別個の契約（コネクテッド・プロダクトのユーザー間サブリースなど）を締結することもできる。

以下の例は、非網羅的な方法で、複数ユーザーシナリオにおけるデータへのアクセス方法を示している。その他のデータ共有の取り決めや仕組みも可能である。欧州委員会が今後発表するモデル契約条項が、さらなる指針を提供することになろう（質問 71 参照）。

例：

サラは 2 週間の休暇でポルトガルに行き、レンタカーを借りる必要がある。レンタカー会社の Sunny Wheels は、大手自動車メーカーの Omni Motors から購入した車を所有している。データ法に基づく権利を行使するため、サラは Sunny Wheels に「コネクテッド・カー」のプロバイダを依頼する。

サニーウィールズはオムニ・モーターズと契約を結び、サニーウィールズとその顧客が車から生成されるデータにアクセスできるようにしている。オムニ・モーターズは、何千人もの車の利用者からのデータアクセス要求を同時に処理できるデータ管理システムを導入している。サラのレンタル契約書には、車から生成されるデータに関する詳細な情報が記載されて

おり、アクセス方法も含まれている。以下は、サラのレンタカーが生成したデータへのアクセスを組織化する 2 つの可能な方法である。

➔ **「法人口座」:** サニーウィールズはオムニ・モーターズの法人アカウントを持っている。サニーウィールズは、オムニモータースのウェブサイトにログインし、レンタカーのデータにアクセスするために必要な詳細をサラにプロバイダする。

➔ **「個別アカウント」:** サニーウィールスはサラに、彼女自身のアカウントを設定し、オムニ・モーターズと個別のデータ共有契約を結ぶ必要があることを通知する。Sunny Wheels は、サラが 2 週間車を使用することを Omni Motors に通知する。

どちらの場合も、オムニ・モーターズは**データ保有者であり、**サニーウィールズはレンタカーを所有し、データにアクセスできるため**ユーザー**であり、サラはサニーウィールズとのレンタル契約により、レンタカーに対する一時的な権利を得たため、**ユーザーでも**ある。

14) ユーザーとして、自分のデータにアクセスするにはどうすればよいか？

第 3 条 2 項は、データプロバイダに対し、その接続製品や関連サービスが生成するデータに関する情報をユーザーに提供する義務を課している。これは「透明性義務」として知られている。

透明性義務の一環として、データ保有者は生成的データへのアクセス方法を利用者に通知しなければならない。データは「直接」（第 3 条 1 項）または「間接」（第 4 条 1 項）に利用可能となる。様々な構成が可能である（例えば、データの一部を直接利用可能にし、残りを間接的に利用可能にすることもできる）。

直接アクセスとは、ユーザーがデータ保有者に要求することなく、当該データにアク セス、ストリーミングまたはダウンロードする技術的手段を有することを意味する。例えば、コネクテッド・プロダクトは、ユーザーがアクセス・メカニズムを管理し、インターフェイスとワークフローを制御し、コネクテッド・プロダクトから直接データを抽出できるデジタル・インターフェイスを有する。

間接的アクセスとは、接続された製品または関連サービスが、利用者がデータ保有者にアクセ スを求める（すなわち承認プロセス）ことを必要とするように設計されていることを意味する。例としては、ユーザーがデータへのアクセス要求を提出できるウェブポータルがある。

第 3 条は、製造事業者が直接アクセスできるように設計するかどうかを決定する際に、ある程度の柔軟性（「関連性があり、かつ技術的に実行可能な場合」）を残している。なぜなら、全ての製品（及び全てのデータ）が利用者が直接データにアクセスできるよう に設計されているわけではないからである。データ保有者がデータへの間接的なアクセスを提供することを好む状況もあり得る。データ法は、データ保有者が利用者にデータを利用可能にする義務を遵守しなければならない場合に、データ保有者にとって最適な解決策を講じることを奨励している。

15）データ法は GDPR のデータ・ポータビリティの権利をどのように補完するか？

すなわち、第 4 条と第 5 条（IoT デバイスからのデータにアクセスし共有する権利）は GDPR 第 15 条と第 20 条（個人データにアクセスしポートする権利）を補完するものである。説明 35 はこの相互関係をさらに明確にしている。

データ法は GDPR 第 20 条で定められたデータ・ポータビリティの権利を補完するものである。GDPR の下では、データ対象者のみがこのような権利を行使でき、個人データが一定の法的根拠（同意または契約）に基づいて処理され、技術的に可能な場合に限られる。データ法は、IoT の文脈に特化した強化されたポータビリティの権利を創設している。データ法のおかげで、ユーザー（データ対象者や企業など）は、コネクテッド製品や関連サービスの使用によって生成されたあらゆるデータ（個人および非個人）にアクセスし、ポータビリティを行うことができる。これは法的根拠とは無関係に、また該当する場合はリアルタイムで行うことができる。したがって、データ対象者は、管理者（例えば、修理・保守サービスを提供する事業体）間で個人データをより容易に移動させることができる。

16）どのような状況で、ユーザーは非個人データを収益化できるか？

利用者は、データ保有者またはサードパーティと自由に契約を締結することができる。データ保有者は、商業目的も含め、利用者の非個人データへのアクセスおよびその利用に対して補償を行うことができる。説明 25 は、企業対企業の関係では、データ保有者と利用者の間の取り決めには、利用者の権利の制限が適切に補償されることを条件に、利用者がデータをさらに使用または共有する権利の放棄を含むこともできると説明している。

17）データへのアクセス権とデータ使用権が適切に行使されない場合、ユーザー、特に消費者にはどのような選択肢があるのだろうか？

データ法は高水準の消費者保護を保証するものである。第 1 条 9 項では、データ法は EU の消費者法、特に不公正契約条件指令（指令 93/13/EEC）、不公正商行為指令（2005/29/EC）、消費者の権利指令（2011/83/EU）を補完するものであり、これを損なうものではないと規定している。

したがって、データ法に基づく権利の行使を求める人々には、いくつかの選択肢が用意されている。

- 利用者（消費者を含む）は、関連する管轄当局に苦情を申し立てることができる。具体的にどの管轄当局に申し立てればよいかわからない場合は、まず加盟国のデータ調整機関に問い合わせるべきである（欧州委員会は、データ調整機関の名前と連絡先をオンラインで公開する予定である）。詳細は質問 64 を参照のこと。
- ユーザー（消費者を含む）は法的手続きを開始することができる。
- 消費者である利用者は、EU の消費者保護法に基づいて利用可能な手段を利用することができる。特に、データ保有者が消費者の居住する加盟国とは別の加盟国に設立されている場合には、欧州消費者センター・ネットワークに苦情を申し立てることができる。

- データ対象者であるユーザーは、個人データの処理に関するすべての問題について、関連する DPA に問い合わせることができる。

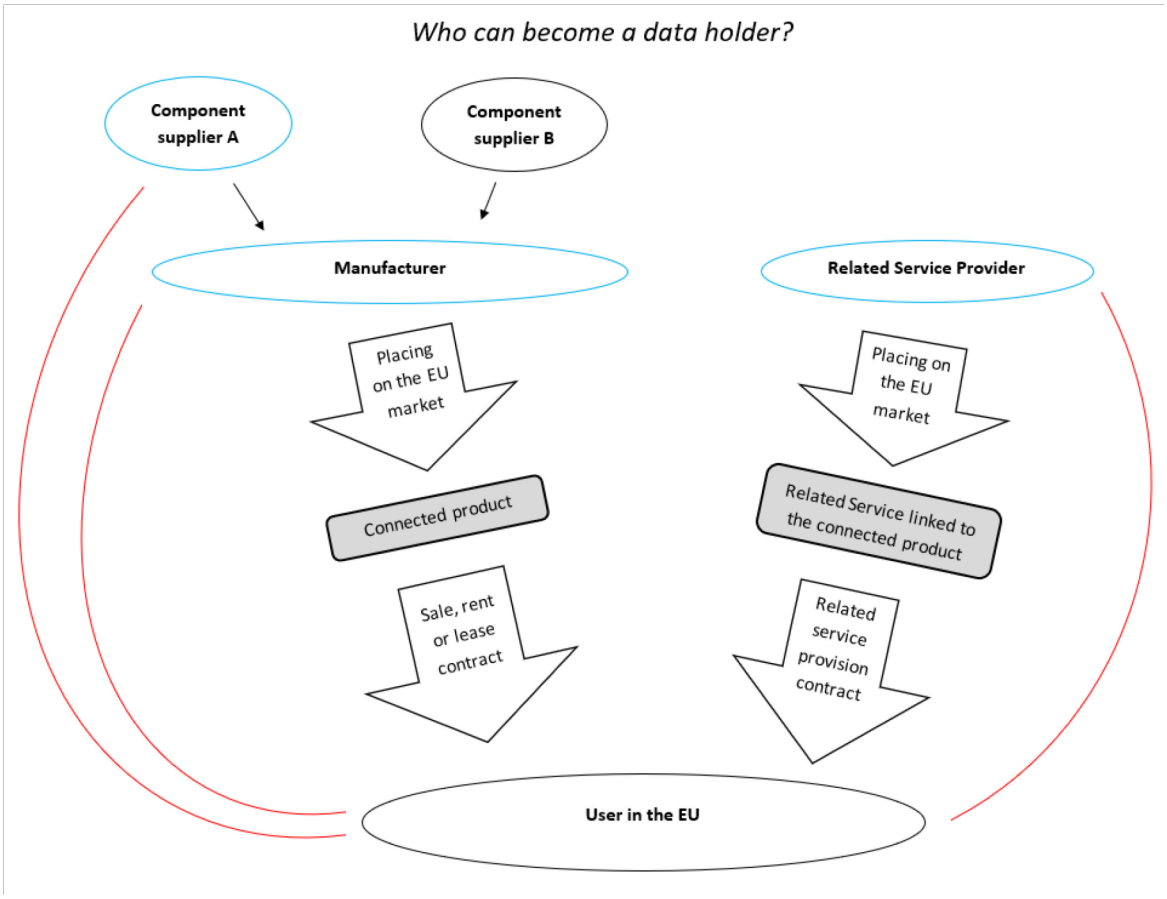
データ保有者に関するセクション

18）製造事業者は常にデータ保有者か？

製造事業者は通常データ保有者であるが、必ずしもそうではない。データ法は、事業体が「データ保有者」の役割を「外部委託」することを認めている。例えば、製造事業者は、その製造事業者の接続製品の全部または一部の「データ保有者」としての役割を他の事業体に委託することができる。

さらに、製造事業者でないデータ保有者は、コネクテッド・プロダクトに結びついた関連サー ビスを提供する企業である可能性がある。つまり、関連サービスを提供する企業がデータ保有者であり、実際にコネクテッド・プロダクトを製造した企業とは異なる可能性がある。

データ保有者が誰であるかを決定することは、ハードウェアやソフトウェアを誰が製造したかに依存するのではなく、容易に入手可能なデータへのアクセス管理を誰が行っているかに依存する。役割分担の例として以下のフローチャートを参照のこと。



このフローチャートは、ユーザーが 2 つの契約（例えば、関連製品の販売と関連サービスの提供）を締結し、ユーザーと 3 つのデータ保有者（青で囲んだ部分）との間に法的関係（赤で囲んだ部分）が成立する状況を示している。利用者は、このような契約を締結する前に、必ずデータ保有者の身元を知らされていなければならない。

1. 製造事業者はデータを受領し使用することに関心があるため、第 3 条 2 項および第 4 条 13 項に従い、販売契約において自らをデータ保有者として定める。

2. 部品供給業者 A と部品供給業者 B は、ともにデータ生成的な部品を納入している。しかし、（B とは異なり）A だけが、その部品によって生成的なデータを受け取り、使用することを望んでいる。供給業者 A が製造事業者から受領したデータを使用できるのでなければ、ユーザーと製造事業者の間で締結された契約に従って、供給業者 A はデータ保有者となり、第 4 条 13 項に従ってデータの使用についてユーザーと合意する必要がある。

3. 利用者が接続製品に関連する関連サービスも取得する場合、関連サービスのプロバイダは、第 3 条 3 項および第 4 条 13 項に従って、必ず利用者と契約を締結しなければならない。したがって、関連サービスのプロバイダはデータ保有者となる。

19）第 3 条 1 項は、コネクテッド製品の製造事業者に対し、ユーザーがデータに直接アクセスできるよう、コネクテッド製品を設計または再設計することを義務づけるか？

第 3 条第 1 項は、製造事業者に対し、すべての状況およびすべての接続製品について、データへの**直接アクセスを**認めることを義務付けてはいない。データは、「**関連性があり、技術的に実行可能な場合には**」、ユーザーにとって「**直接アクセス可能**」**で**なければならない。

「**関連性があり、かつ技術的に実現可能な場合**」という文言は、ユーザーに「非管理的」アクセス（すなわち、他者による介入なし）を提供する方法でコネクテッド製品を設計するか、（典型的にはリモートサーバーを経由して）追加的な管理を伴うアクセスを提供する方法でコネクテッド製品を設計するかを決定する製造事業者の裁量を強化することを意図している。この目的のために、製造事業者は、例えば、直接アクセスが技術的に可能かどうか、潜在的な技術的修正 のコスト、企業秘密や知的財産の保護や接続された製品のセキュリティ確保の難しさなどを評価することができ る。また、コネクティッド製品、ユーザー、データ保有者の観点から、特定のシナリオにおいて直接アク セスが適切かどうかを検討することもできる。このアセスメントに基づき、製造事業者は、製品データの全部または一部が直接アクセスできるようにコネクティッド製品を設計することを選択することもできるし、間接的なアクセスのみを可能にすることもできる。合意された場合、データ保有者は、ユーザが直接アクセス可能な製品データにアクセスすることもできる。

データが「**直接アクセス可能」で**あるのは、以下のような場合である：

- 利用者は、データ保有者をはじめとする他者の介入なしにデータにアクセスすることができる（これは、データ保有者の介入を必要とする第 4 条および第 5 条に基づく要求に代わるものである）。
- ユーザーは、接続された製品の設計の結果として、データをストリーミングまたはダウンロードする技術的手段を有している。製造事業者またはデータ管理者の管理下にある遠隔地のサーバーから「直接アクセス」することも可能である。

端的に言えば、データが「**直接アクセス可能」**であるためには、データがどこに保存されているかにかかわらず、データ保有者の関与なしに利用者がデータにアクセスできなければならない。直接アクセスが可能でリモートサーバーがある場合でも、データ保有者はユーザーが関連データに容易にアク

セスできる手段（API などの適切なインターフェース）を提供する義務がある（データ法第 3 条 1 項と GDPR 第 20 条を比較した説明 35 参照）。

データ法の施行日（2025 年 9 月 12 日）までに、すでに上市されている製品および新製品（上市時）は、ユーザーがデータにアクセスできるようにしなければならない。この日までに、製造事業者はそのようなアクセスを**直接**行うか**間接的に**行うかを決定しなければならない（第 4 条 1 項参照）。企業は、自社に最適なソリューションの使用を奨励する現実的な方法を見つけるだろう。分野別の法律はより具体的である。

20) 新しいデータアクセス権は営業秘密の保護に影響するか？

データ法は、データ共有とデータの保護された性質を保持する必要性（機密性が引き続き確保される営業秘密の保護を含む）とのバランスをとる枠組みを提供する。データ法は、適用される法的防御（すでに企業秘密保護の法的枠組みを提供している 2016 年企業秘密指令を含む）を修正するものではない。

しかし、データ保有者はどのデータが営業秘密であるかを一方的に決定することができるため、あるデータが営業秘密であると主張するだけでは、データ法が規定するデータアクセス権の行使を妨げるには不十分である。このことは、データ法が営業秘密保護の没収につながることを意味するものではない。むしろ、ユーザーの新たなデータアクセス権に対する違法な制限を防止する必要性と、営業秘密に提供される法的保護を維持する必要性とのバランスを慎重に取っているのである。

従ってデータ保有者は、開示に先立ち、そのために必要な保護措置に同意し実施することで、営業秘密が包含されたデータの機密性と秘密保持を保持するよう利用者とサードパーティに要求する権利を有する。追加の保護として、データ法は、データ保有者がデータを保留、一時停止、または例外的にデータ 共有を拒否できる条件を定める新しい仕組み（一般に「営業秘密ハンドブレーキ」として知られ ている）を導入している。

データ保有者は営業秘密をどのように扱い、「営業秘密ハンドブレーキ」を作動させることができるか？

データ保有者はデータへのアクセス要求を受けた場合、共有が必要な営業秘密を**特定**し、その秘密保持のために必要な措置について利用者／サードパーティと**合意**しなければならない（第 4 条(6)および第 5 条(7)）。これらの保護措置は、データの共有に先立って実施される必要がある。考えられる措置としては、モデル契約条項、秘密保持契約、厳格なアクセスプロトコル、技術標準、行動規範の適用などがある。

データ保有者は、合意がない場合、ユーザーまたはサードパーティが合意された措置を実施しない場合、または営業秘密の機密性が損なわれる場合、営業秘密の共有を**保留**または**停止**することができる（第 4 条(7)および第 5 条(10)）。

例外的状況において、データ保有者は、客観的証拠に基づき、営業秘密の開示によって重大な経済的損害が生じる可能性が高いことを証明できる場合、営業秘密の共有を**拒否する**ことができる（第 4

条(8)および第 5 条(11))。深刻な経済的損害」とは、深刻かつ回復不能な経済的損失を意味する。このような判断はケースバイケースで行う必要がある。

データ保有者がデータ共有の保留、停止、拒否を検討する場合、加盟国の認定機関に**通知**し、過度な遅滞なくその決定の理由を利用者またはサードパーティに伝えなければならない。

利用者またはサードパーティは、加盟国の裁判所または法廷に救済を求め、データ保有者の決定に異議を申し立てることができるほか、紛争解決機関に問題を付託することにデータ保有者と合意することもできる。利用者または第三者は、管轄当局に苦情を申し立てることもできる。管轄当局は、データ共有を開始するか再開するか、またどのような条件の下で開始するかを、過度の遅滞なく決定しなければならない（第 4 条 9 項および第 5 条 12 項）。

21) 営業秘密の保護は、第 3 条(1)の意味で直接入手可能となったデータに関しても適用できるか？

データ法は、接続された製品（または関連サービス）を設計する際に、容易に入手可能なデー タをユーザーが直接、間接、またはその両方の組み合わせでアクセスできるようにするかどうかを製造事 業者が選択できることをまず強調しておくことが重要である（質問 14 参照）。特に、直接アクセスの場合、ユーザーがどのようにアクセス権を行使するかについて、間接アク セスの場合よりも製造事業者はあまり関与しない（または全く関与しない）ことになるため、このような 選択をする場合、営業秘密の保護が考慮事項となり得る。

しかし、直接アクセスは無条件でなければならないという意味ではない。製造事業者は、営業秘密の保護を確保するために、直接アクセス可能な特定のデータを保護することを契約上ユーザーに義務付けることができる。第 4 条(7)、第 4 条(8)、第 5 条(10)及び第 5 条(11)の考慮事項（「営業秘密のハンドブレーキ」と呼ばれる）に基づ いて直接アクセスを無効にすることはデータ法によって禁止されているわけではなく、契約に基づいて交渉 されるべき問題である。そのような契約条件は、第 7 条 2 項に従って、利用者の権利を損なうことはできない。

それにもかかわらず、データ法が施行される前に締結された契約で合意された直接アクセスに関す る契約義務を再交渉する論拠としてデータ法を持ち出すことは不適切であると思われる。データ法は、レガシー製品やそれぞれの契約上の合意の営業秘密の保護に関して状況を変えるものではない。

22) 安全／セキュリティ上の懸念がある場合、データ保有者はデータを共有しなければならないか？

データ法第 4 条 2 項に従い、接続された製品のセキュリティ要件が損なわれ、人々の健康、安全またはセキュリティに重大な悪影響を及ぼすリスクがある場合、利用者とデータ保有者はデータの共有を制限または拒否することに合意することができる。このような要件は、EU 法または国内法に定められていなければならない。部門認可は、制限が必要か正当かを判断するために、ユーザーやデータ保有者に技術的な専門知識を提供することができる。

このメカニズム（すなわち、安全性やセキュリティの考慮に基づいてデータアクセスを制限または禁止する可能性）は、「安全性とセキュリティのハンドブレーキ」と呼ばれている。

上記に説明した条件下で、データ保有者がこのハンドブレーキを作動させようとする場合、データ保有者は各加盟国の認定機関に通知しなければならない。さらに、利用者は、データ保有者によるデータ共有拒否に対して、管轄当局、裁判所、紛争解決機関に異議を申し立てることができる。

23）関連商品に対する競業避止条項が導入された。これは関連サービスにも適用されるか？

データ法の主な目的は、サービスプロバイダーが新しいデータにアクセスし、製造事業者が提供する同等のサービスと対等に競争できるようにすることである。競合する関連サービスの開発を禁止することは、技術革新や他のサービス（必ずしも「関連サービス」ではない）の提供に抑制的な影響を与える可能性がある。

非競争条項が接続製品のみに限定された結果、企業と消費者は、代替サービスへの切り替えコストが削減されることになる。また、このようなデータへのアクセスに依存する付加価値サービス（予知保全など）の競争が激化し、より多くの情報に基づいた消費者の意思決定（より持続可能な製品やサービスの購入など）が可能になる。

24）データ保有者の利益はどのように保護されるか？

データ保有者の利益はさまざまな方法で保護されている。以下に 4 つの例を挙げる。

i. データ法は、第 II 章に基づく強制的共有義務の対象となるデータの範囲を、生データと加工前データに限定している。これにより、データ関連投資や企業秘密・知的財産権の保護への悪影響を最小限に抑えることができる。

ii. 具体的な規定は、利用者が要求したデータがデータ保有者／企業秘密保有者によって企業秘密とみなされる場合や、データの利用がかなりの安全リスクと関連する場合に対処するものである。

iii. データ法に基づくコネクテッド製品からのデータアクセスは、競合製品の開発に使用することはできない。

iv. データ保有者は、サードパーティ（ユーザーからデータ共有を促された場合）またはデータ取得者（法的なデータ共有義務がある場合）に補償を要求することができる。

25）データ法は、EU 域外に設立されたコネクテッド製品の製造事業者や関連サービスのプロバイダに適用されるか？

データ法は、製造事業者または関連サービスプロバイダーが EU に設立されていることを要求していない。データ法は、EU 域内のユーザーが容易に入手可能なデータにアクセスし、使用し、共有する権利を定めている。したがって、EU 域内に設置されるすべての接続製品および関連サービスは、この権利を行使できるように設計されなければならない。

すべての法的要件は、接続製品が EU 上市されるとき、または関連サービスが提供されるときに満たされなければならない。関連サービスはコネクテッド・プロダクトの機能と連動しているため、関連サービスのプロバイダの設立地は、データ法の適用範囲に入るか否かを決定する要因にはならない。

26) 利用者が生成したデータをデータ保有者が使用することに制限はあるか？

GDPR はパーソナルデータの処理を規定しているが、データ法第 4 条(13)および(14)はデータ保有者による非パーソナルデータの使用を対象としている。

第 4 条(13)は、(i)これがユーザーと合意されていること、(ii)データ保有者が、ユーザーが活動する市場におけるユーザーの商業的地位を損なう可能性のあるその他の方法で、ユーザーの経済状況、資産および生産方法に関する洞察を導き出さないことを条件として、データ保有者が個人データ以外のデータをいかなる目的にも使用できることを規定している。

Recital25 はさらに、データ保有者が意図するデータ使用に関する契約条項は、利用者に透明でなければならないと規定している。データ保有者によるデータ使用の機能改善には、接続された製品または関連サービスの機能改善や、集計されたデータをサードパーティが利用できるようにすること が含まれる。ユーザーは、接続製品または関連サービスから得られる粒度の細かい非個人データにアクセスする唯一の情報源である。

第 4 条(14)は、データ保有者によるデータ利用の具体的な側面として、個人データ以外のデータを第三者と共有することを取り上げており、これは（第 4 条(13)と同様に）利用者と契約上合意した場合にのみ行われるべきである。

27) データ保有者は、正当な利用者をどのように確認できるか？

第 4 条 5 項は、利用者である可能性のある個人を確認するために、「プロバイダは、その個人に対し、必要以上の情報の提供を要求してはならない」と規定している。説明 29 は、「データ保有者は、利用者がデータにアクセスする権利を有することを確認するために、適切な利用者の識別を要求することができる」と説明している。

したがって、ユーザが提供を求められる「情報」は、その人がユーザであること（すなわち、「接続された製品を所有しているか、その接続された製品を使用する一時的な権利が契約上譲渡された人、または関連するサービスを受ける人」（第 2 条(12)）であることを決定的に証明するものでなければならない。データへのアクセスというユーザーの既得権益を考えれば、ユーザーが自分自身を適切に識別しようとすることを期待するのは合理的である。

付属文書 21 は、データ保有者がどのようにユーザーを確認するかについてのガイダンスを示している。このリサイタルによると、アクセスは利用者に付与されるべきである：

> 自動実行を認め、製造事業者またはデータ保有者による審査または許可を 必要としない簡単な要求メカニズムに基づく。*(*中略*)* データアクセス要求の自動実行が、例えば、接続された製品または関連サー ビスと共に提供されるユーザーアカウントまたは付随するモバイルアプリケー

ションを介 して不可能な場合、製造事業者は、データへのアクセス方法についてユーザーに通知すべきである。

従って、データ保有者は利用者を特定するための具体的なプロセスを自由に設定することができるが、それでも第 4 条(4)及び(5)を遵守しなければならない。データ保有者は、例えば、(i)製品の種類、(ii)利用者の種類（消費者対産業）、(iii)利用者の数（エレベ ーターの所有者対レンタカーの複数の利用者）、(iv)予想されるデータアクセス要求の頻度、(v)所有権を証 明する具体的な仕組み（車の所有者登録など）の有無、(vi)差別化された利用者アカウントの設定コスト、(vii)実 際の利用者にとってそのようなアカウントの使いやすさなどを評価することができる。該当する場合、EU デジタル ID ウォレットのようなソリューションが想定される。

個人データに関して、34 項では、「個人データは、データ管理者またはデータ対象者によってのみ要求することができる（...）ユーザーがデータ対象者ではなく、個人事業主を含むエンタープライズであり、接続製品を家庭で共同使用する場合ではない場合、ユーザーは管理者であるとみなされる」と説明している。

説明 34 は、データ対象者であるユーザーは、常に自分自身に関する個人データにアクセスできることを想起させる。また、データ対象者でないユーザーは GDPR 上の管理者であり、IoT デバイスから個人データを要求する際には GDPR 上の義務を遵守しなければならないことを明確にしている。

28）データ保有者は、ユーザーへの直接アクセスを許可している場合でも、ユーザーの要求に応じて第三者とデータを共有する必要があるか？

はい。利用者が第 3 条 1 項の意味においてデータに直接アクセスできる場合、利用者は第 5 条に基づき、データ保有者に対して第三者へのデータ移転を要求する権利も有する。これは、利用者が容易に入手できるデータを持つデータ保有者が存在することを前提とする。第 5 条は、利用者がどのようなアクセス権を持っているかを条件としていない。

29）ユーザーは、データ保有者が保存しているかもしれない過去のデータへのアクセスを要求できるか（例えば、中古のセンサー／機械を購入する場合）。

データ法は、接続されたオブジェクトの使用によって生成されたデータ（自分より前に他のユ ーザーによって生成されたデータを含む）にアクセスし、容易に利用できるようにする権利をユーザーに与え ていると読み取ることができる。そのような後発の利用者は、説明 24 で言及されている「合理的な保持方針」を念頭に置きつつ、そのようなデータに対して（例えば更新やインシデントに関して）正当な利益を有する可能性がある。

しかし、以前の利用者の権利やその他の適用法（例えば、個人データや商業上の機密情報に関して、データの削除要求を含む）は尊重されなければならない。その意味で、「履歴データ」の粒度や範囲は、他者の権利や利益を保護するために制限される。

30）ユーザーは、他のユーザーに製品を販売する前に、データ保有者に対して自分の非個人データの削除を要求できるか？

データ法は、GDPR のような非個人データに対する具体的な「忘れられる権利」を定めていない。しかし、当事者が契約上、関連製品の販売前にデータを消去する可能性について合意することを妨げるものはない。これが合意された場合、データの消去方法に関する情報は、第 3 条 2 項(d)に従った要求事項の一つであり、また、説明 21 は、複数の利用者がいる場合のアカウントソリューションに関するガイダンスを示しており、そこでは、利用者は自分のアカウントに関連する非個人データを消去することが認められるべきである。同時に、製品によっては、分野別の法律で異なる規定がなされることもある（例えば、ある種のデータが安全上の理由から製品に「従う」ことを意味する場合など）。

31）企業はユーザーであると同時にデータ保有者でもあり得るか？

第 2 章では、企業は同一のデータについてユーザーとデータ保有者を兼ねることはできない。しかし、異なるコネクテッド・プロダクトや関連サービスに関しては、ユーザーとデータ保有者を兼ねることができる。例えば、製造事業者は、その工場で使用されるロボットの「ユーザー」であると同時に、その工場で製造されるコネクテッド製品の「データ保有者」でもあり得る。）

加えて、データ法は、データ保有者がいなくても、個人をコネクテッド製品のユーザーとすることを認めている。例えば、データが機器に直接保存されたり、機器からユーザーのコンピュータに転送されたりするコネクテッド製品をユーザーが購入し、製造事業者がそのデータに一切アクセスできない場合、データにアクセスできるのはユーザーのみであるため、データ保有者は存在しない。

サードパーティに関するセクション

32）第Ⅱ章の文脈において、サードパーティはユーザー／データ保有者から受け取ったデータで何ができるか？

第 6 条 1 項の一般原則は、サードパーティはユーザーと合意した目的（通常はユーザーへのサービス提供）のためにデータを使用できるというものである。第 6 条 2 項には、サードパーティが禁止する行為のクローズドリストが含まれている。このリストには、競合製品を開発するためにデータを使用することや、ゲートキーパー（デジタル市場法で定義されている）とデータを共有することが含まれている。

33）利用者はデータ保有者に対して、デジタル・マーケット法のゲートキーパーとデータを共有することを義務付けることができるか？

DMA ゲートキーパーは、デジタル市場法（DMA）に基づきコアプラットフォームサービスを提供するプロバイダと定義され、通常、大量のデータにアクセスすることに困難はない。ゲートキーパーの地位、プラットフォーム・エコシステムに対する支配力、優れた交渉力により、データはすでにこのような大企業に引き寄せられる傾向にある。従って、DMA ゲートキーパーとの IoT データ共有を義務付けることは、遵守しなければならない人々にとって不公平であり、データ法の目的からすれば不必要である。したがって、DMA ゲートキーパーは、データ法に基づき新設された IoT データアクセス権の意味でのサードパーティにはなり得ない。

これは、DMA ゲートキーパーが IoT（データ）市場から完全に排除されることを意味するものではない。DMA ゲートキーパーは、第 4 条と第 5 条によって創設された特定の強制的データ共有メカニズムに依存することは禁止されている。他のすべてのメカニズム（自発的なデータ共有の取り決めを含む）は影響を受けないままである。

34）第二章のデータ共有義務に基づき、第三国に設立された者がデータを受け取ることは可能か？

データ保有者に対する第 2 章のデータ共有義務の範囲は、EU 域内の事業体および消費者を含む個人に限定されている（第 1 条 3 項（b）、1 条 3 項（d）および 2 条 14 項参照）。EU 域内に拠点を持たない事業者にデータへのアクセスを与えることは、データ法に基づいて正当化することはできない。

データ保有者は、その設立地に関係なく、EU ユーザーの要求があれば、EU に拠点を置く事業体または個人とデータを共有する法的義務を負う。ユーザーは、EU に設立されていない事業体または個人とデータを共有するようデータ保有者に要請することができるが、データ保有者はその要請を承諾する義務はない。

公正、合理的かつ非差別的（FRAND）な条件、補償、紛争解決

35）データの取得者を区別し、異なるライセンス条件を適用することは可能か？

第 8 条 3 項は、同じ状況にある事業体を区別することは許されない（無差別）という一般原則を実施している。2 つの取得者が同等のカテゴリーに属するかどうかの分析は、ケースバイケースで行わなければならない。

36）妥当な報酬に上限はあるか？

報酬に上限（下限）はない。むしろ、データ法は報酬の算定が一定の客観的規準（例えば、かかった費用や利用可能になるデータ量）に基づくことを保証するために、一定の透明性要件を課している。取得者が中小企業や非営利の研究機関である場合、合理的な報酬に利益率を含めることはできない。

37）誰が、どのような条件の下で、データ法によって確立された紛争解決メカニズムに頼ることができるか？

利用者、データ保有者、データ取得者は、データ法に従って加盟国が指定する紛争解決団体に紛争を付託することができ、紛争解決団体はデータ共有に関する契約の締結や契約締結後に生じた紛争の解決を支援することができる。これらの紛争解決機関は、(i)企業対消費者、企業対企業の関係における「安全・安心のハンドブレーキ」と「企業秘密のハンドブレーキ」（質問 20、21、22 参照）に関する紛争、(ii)データ利用のための公正、合理的、非差別的条件に関する紛争、(iii)データ共有のための公正、合理的、非差別的条件に関する紛争、(iv)データ共有のための公正、合理的、非差別的条件に関する紛争、(v)データ共有のための公正、合理的、非差別的条件に関する紛争を管轄する、また、(iii) 企業間関係におけるデータへのアクセスおよび使用に関する契約条件の公正さ に関する紛争である。

紛争解決規則は、データ共有の義務が（データ法そのものを含む）適用法に明記されている企業間関係において、データを利用可能にするための（透明性のある）公正で合理的かつ非差別的な条件に関連する紛争に適用される。紛争解決規則は、データ処理サービスの顧客とプロバイダが、そのようなサービスに関するデータ法の規定違反に関連する紛争を解決するために使用することもできる。

紛争解決機関に訴える決定は任意であり、紛争当事者双方によって合意されるべきである。さらに、紛争解決機関の決定は、紛争解決手続の開始前にその拘束力について明確に同意した場合にのみ、団体を拘束する。

紛争解決機関は、紛争がすでに他の紛争解決機関に提訴されている場合、または加盟国の裁判所もしくは法廷に提訴されている場合、その解決を命じられてはならない。

企業間データ共有契約における不公正

38) 中小企業は往々にして交渉上の立場が弱いことを踏まえ、中小企業を支援するためにどのような特別規定が存在するか？

第 4 章では特に中小企業を取り上げていないが、不当な契約条件の禁止は、契約条件が一方的に押し付けられた企業に利益をもたらすと予想される。

中小企業は市場支配力が限定的で交渉力も弱いことが多いため、第 4 章では、特に大企業が保有するデータへのアクセスを求める場合に、中小企業に対する特別な支援を提供する。中小企業が苦情を申し立てたり懸念を表明したりする必要がある場合は、例えば加盟国のデータ・コーディネーターに連絡することができる（質問 64 に対する回答を参照）。

欧州委員会は、データ法の権利と義務を反映し、中小企業がより良い交渉を行えるようにすることを目的とした、データ共有に関するモデル契約条項を推奨する。これらのモデルは任意である。欧州委員会は、データ法の適用が開始されるまでにこれを採択する予定である。

39) 契約書のデータ共有契約条項が不当だと思う。どうすればいいか？

まず第一に、問題の用語がデータ法第 13 条の対象であることを確認する必要がある：

a) これらは、データへのアクセスとその使用、あるいはデータ関連義務の違反や終了に対する責任と救済措置に関するものである；

b) これらの条項は、EU 法の強行規定、または契約条項がその事項を規制していない場合に適用される EU 法の規定を反映していない；

c) 一方的に押し付けられたものである。

d) 契約の両当事者はエンタープライズである。

第二に、その条項がデータへのアクセスやデータ利用における善良な商慣行から著しく逸脱し、誠実かつ公正な取引に反しているかどうかがアセスメントされなければならない。このような条項の非排他的リストは第 13 条(4)にプロバイダとして規定されている。このような条件は常に不公正とみなされるべきである。

第三に、問題の条件は別のカテゴリーに分類される場合がある。すなわち、不公正であると推定されるだけの条件である。不当な条件を課す側は、それに反する証拠を提示することによって、そのような推定を覆すことができる。このような条件は第 13 条(5)に列挙されている。

上記のアセスメントの結果、契約条項が不当である、または不当であると推定されることが確認された場合、そのような条項を課す当事者は契約から離脱するよう求められるべきである。いずれにせよ、不当と判断された条項は、それが課された当事者を拘束することはない。残りの契約条項は、不当な条項をそれらから切り離すことができれば（すなわち、十分に独立したものであれば）、拘束力を持ち続ける。

認可当事者がアセスメントの結果に異議を唱え、条件を撤回しない場合、この問題は管轄当局、裁判所、または（相手側が同意すれば）紛争解決機関に提訴することができる。

企業対政府のデータアクセス

40) 何が「公共緊急事態の低減または復旧」に該当するか？

データ法はこれらの概念を明確にしていないが、第 15 条はこれらを「公的緊急事態への対応」と明確に区別しており（第 15 条 1 項(a)）、特に時期の点で、公的緊急事態の実際の発生とは異なることを示唆している。ある活動を「公的緊急事態の軽減または回復」と特定する際に考慮すべき要素は、国内法に定められている可能性が高い。なぜなら、公的緊急事態の軽減または回復が第 V 章の要請に関連するためには、「公共の利益のために実施され、法律で明確に規定された特定の業務」として指定されなければならないからである。

41) 第 15 条 1 項（a）において、「同等の条件」とは何を意味するか？

同等の条件下で」は、本条の文脈では、第 V 章に基づく権利の行使を希望する公的機関に対し、まず同じデータが他の場所で入手できないかどうかを検証することを要求する規則として読み取れるが、同時に同等の労力を要求することになる。この点については、レシタル 64 の最後の文にいくつかの例が示されている。

42) データ法に基づく新しい権利は、公共部門がデータを購入する代わりにデータを要求することができるため、データ保有者の既存のビジネスモデルを危険にさらす可能性があるのだろうか？

現在のビジネスモデルが深刻な影響を受けるリスクはほとんどない。というのも、公共緊急事態に直接対応するためにデータを必要とする例外的な状況以外のすべての状況において、非個人データを購入する選択肢が公共機関にある場合、データは市場価格で購入される必要があるからである（第 15 条(3)の例外に注意）。公的機関が第 15 条(1)(b)の手続きに依拠できるのは、非個人データを入手できなかった場合のみである-データが購入できないか、公的機関が（調達などを通じて）市場価格で購入しようと試みたが失敗したためである。

43) データ保有者は、第 5 章の要請が正当かつ合法的であることをどのように確認できるか？

データ保有者は以下を確認すべきである：

- 要請事業体は加盟国の公的機関か、または第 17 条(1)に列挙されている EU レベルの事業体か？
- データ保有者の選択、特定のデータの範囲、例外的な必要性の存在、使用期間、公的任務の性質、データ要求の目的（第 17 条(1)(a)～(j)による）について、十分かつ明確な正当性があるか？
- その要請は、説明された例外的な必要性に見合ったもか（データの範囲や粒度など）。
- 個人データを要求する場合、第 17 条 1 項（g）および 17 条 2 項（e）に記載されている必要条件が満たされているか？

- 必要な認定機関はすべて認可されているか（加盟国が異なる公的機関からの要請の場合など）。
- 上記の条件について正当な疑念がある場合、データ保有者は説明を求め、最終的に要求を 拒否するか、またはその修正を求めることができるものとする。このような場合、要求事業体は管轄当局に問題の解決を求めることができる。

44）ある国の公的団体は、異なる国のデータ保有者にデータを要求できるか？その場合、データ保有者の権利は完全に保護されるか？

データ法には、公共部門機関が、要求する公共部門機関の加盟国ではない加盟国に所在するデータ保有者（団体）にデータを要求する権利が含まれている。この権利は、国境を越えた緊急事態（自然災害など）の場合に重要となる。

いつものように、要請は第 17 条のすべての要件を満たす必要がある。つまり、データ保有者が理解できるように、明確で簡潔、かつ平易な言葉で作成されなければならない。

データ法第 22 条には、データ保有者の保護を確保するための国境を越えた要求に関する特別な手続きが含まれている。このような要求は常にデータ保有者の加盟国の認定機関に通知され、事前審査が行われる。

45）要請に応じてデータが提供された場合、それらは公的機関の情報となるか？公共部門団体はそれをどのような形でも利用することができるか？

要請されたデータは、指令（EU）2019/1024（オープンデータ指令）に基づきオープンに再利用可能にしなければならない公共部門の情報にはならない。原則として、データは要求で定められた特定の目的のためにのみ、要求団体によってのみ使用することができる。ただし、要請団体は、データが要請された公共部門の業務を遂行するにあたり、他の公共部門機関またはサードパーティーの関与を必要とする場合がある。その場合、関連する公的機関またはサードパーティは、第 17 条(1)(f)に従い、要請の中ですでに特定されていなければならない。

第 21 条は、要求されたデータが他と共有される 2 つの状況について述べている：(i) データが要求された目的に適合する科学的研究または分析を実施するため、および(ii) 公的統計を作成するため。このような移転が行われた場合、データ保有者は認定機関に苦情を申し立てる機会を与えられるよう、通知されるべきである。

第 21 条に記載されたメカニズムの下で共有されたデータは、データが要求された当初の目的が達成されてから 6 ヶ月以内に削除されなければならない。

46）第 V 章に基づく要請は、異なる公共団体によって反復的または同時に行うことができるか？

データ保有者は、同じデータに対する反復的な要求に対応することは期待できない。公共団体 はまず、そのデータが公共部門内ですでに利用可能かどうかを確認すべきである。したがって、データ法

は、(i)同じ目的の同様の要求が他の公的機関、欧州委員会、欧州中央銀行、または他の EU 機関から以前に提出されており、(ii)データ法第 19 条(1)(c)に従ってデータ保有者がデータの消去について通知を受けていない場合、データ保有者に要求を拒否する権限を与えている。

47) 第 5 章が政府によって利用され、市民の基本的権利が危険にさらされる可能性はあるのだろうか？

共同立法者は、公的機関が意図せずとも市民や企業の権利をリスクにさらす可能性を制限するため、第 5 章の条文を慎重に起草した。具体的な規定は、例外的な必要性によって正当化されるデータ要求の必要性が、いかなる形であれ個人データや企業秘密の保護を低下させないことを保証するものである。これらの規定には主に、有効な要求の要件が詳細に列挙された第 17 条、第 18 条 4 項、第 19 条 1 項(b)および第 19 条 3 項～4 項が含まれる。

データ法第 5 章の規定に違反する疑いがある場合は、関連する裁判所またはデータ保有者が設立されている加盟国の管轄当局に提訴することができる。

48) 公共部門団体は、第Ⅱ章におけるコネクテッド・プロダクト／関連サービスの「ユーザー」となり得るか？

そうだ。公共部門団体が（別個の事業体として）第 2 章の意味での利用者になることを妨げるものはない（説明 18 参照）。

データ処理サービスの切り替え

49）第 VI 章の適用範囲から除外されるサービスは何か？

第 23 条から第 32 条および第 34 条から第 35 条は、データ処理サービスのプロバイダに適用される。データ処理サービスの定義は第 2 条 8 項に規定されており、クラウドコンピューティング・サービスの一般的な定義を反映している。この概念は、一般的な提供モデルである IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）をカバーするように設計されており、同時に技術革新にも対応できるようになっている。

第 31 条は、(i)カスタムメイドで広範な商業規模で提供されないデータ処理サービス、および(ii)テスト版／ベータ版として提供されるデータ処理サービスに対する特定の制度を導入している。ただし、これは特注サービスが第 6 章の適用範囲から完全に除外されることを意味するものではない。第 31 条第 1 項に列挙されていない規定は依然として適用される。例えば、このようなサービスのプロバイダは、オープンなインタフェースを利用できるようにし、データが構造化され、一般的に使用され、機械で読み取り可能な形式でエクスポートされるようにしなければならない。

50）輸出可能なデータとデジタル資産の違いは何か？これらの概念は何を意味するか？

第 2 条(38)によれば、「輸出可能なデータ」の概念には入力データと出力データが含まれる。また、顧客が各データ処理サービスを利用することによって直接的または間接的に生成された、あるいは共同で生成されたメタデータも含まれる。これらの概念は、プロバイダまたは第三者の知的財産および企業秘密として保護されるデータを除外する。

「デジタル資産」は第 2 条(32)で定義されている。デジタルアセットとは、顧客が乗り換えた新しいプロバイダの環境でデータを効果的に利用できるようにするために必要な要素である。従って、デジタル資産には、例えば、設定、セキュリティ、アクセス権・管理権の構成に関するものなど、他の種類のメタデータも含まれる。アプリケーションだけでなく、仮想化技術（仮想マシンやコンテナなど）もデジタル資産としてカウントできる。切り替えプロセスの一環として、顧客が切り替えようとするデータ処理サービスのプロバイダとの契約関係とは無関係に、顧客がこれらの資産を使用する権利を有している場合、デジタル資産を切り替え元のプロバイダから切り替え先のプロバイダに移植することができる。

51）プロバイダがスイッチング料金を削減し、プロバイダが負担するコストに限定できるようにする期限は？

第 29 条 2 項に従い、データ処理サービスのプロバイダは、2024 年 1 月 11 日以降、スイッチング料金（イグレス料金を含む）を削減しなければならない。具体的には、プロバイダーはスイッチング料金を、スイッチングを行うために発生する費用に限定しなければならない。2027 年 1 月 12 日以降、プロバイダはスイッチング（データ消去を含む）料金を請求できなくなる。

特別なルールが適用されるのは、顧客が乗り換えを行わず、代わりにプロバイダに他のサービスと並行してサービスを提供するよう依頼する場合である（マルチクラウドの展開モデルなど）。このような

並行利用の場合、プロバイダは 2027 年 1 月 12 日以降も、データのイグレスに発生したコストを顧客に請求することができる。これは、マルチクラウドの展開が、スイッチング運用で予想される単発のデータ排出とは対照的に、恒常的なデータ排出を意味する場合があるためである。

52) 「フリー・ティア・オファー」とはどういう意味か？

第 23 条(c)は、フリーティア・オファリングの恩恵を受けた顧客もスイッチングの恩恵を受けられることを明確にしている。フリーティア・オファリング（クラウドクレジットと呼ばれることもある）とは、プロバイダから顧客へのデータ処理サービスの無償提供のことである。フリーティア・オファリングは、顧客がデータ処理サービスをテストしたり、新興企業を支援したりすることを目的としている。

53) 通知期間と移行期間はどのように関係するか？

第 25 条は、顧客がデータ処理サービスのプロバイダに対し、他のプロバイダまたはオンプレミスの ICT インフラへの切り替えを希望する旨を通知した時点で、通知期間が開始すると定めている。切り替えは、通知期間終了後に開始される移行期間（最長 2 ヶ月）の終了までに完了する必要がある。

移行期間中（最大 30 暦日）、プロバイダは、顧客の切り替えを可能にするために必要な措置を、顧客自身および該当する場合は顧客の新しいプロバイダと緊密に協力して実施しなければならない。顧客は、30 日間の移行期間をより長い期間に置き換える権利を有する。プロバイダが移行期間を延長できるのは、通知期間中の 14 日以内に、最大 30 日の移行期間が技術的に不可能であることを証明できる場合のみである。この場合、移行期間は最長 7 ヶ月となる。

54) 欧州委員会は、データ処理サービスの相互運用性を確保するための連邦共通のリポジトリをどのように構築するか？

そのプロセスは第 35 条に定められている。

リポジトリはオンライン・プラットフォームの形をとる。このリポジトリは、プロバイダが提供するサービスの種類に適用される標準または共通仕様（オープンな相互運用性仕様に基づく）を確認するためのワンストップ・ショップとなる。プロバイダは、顧客がアクセスできるようにするインターフェースが、リポジトリで参照されている標準／仕様と互換性があることを保証しなければならない。その目的は、クラウドサービスの相互運用性を確保することで、顧客が機能を失うことなく切り替えの恩恵を受けられるようにし、プロバイダが切り替えプロセスにおいて顧客をサポートしやすくすることである。

まず第一段階として、欧州委員会は、既存の標準規格や相互運用性に関するオープンな仕様のうち、このリポジトリで承認される資格のあるものをマッピングする。欧州委員会は、整合標準や共通仕様をリポジトリに登録する前に、実施法を採択しなければならない。マッピングに続く次のステップは、実施法の作成であり、これはコミトロジー手続きの中で採択される。

このリポジトリは生きた文書であり、関連する新しい標準やサービスタイプごとの共通仕様で継続的に更新される。

55) クラウド・コンピューティング契約の標準契約条項の現状はどうなっているのだろうか？

データ法第 41 条に基づき、JUST 総局と CNECT 総局が共同で運営する B2B データ共有とクラウドコンピューティング契約に関する専門家グループは現在、データ共有のモデル契約条項とクラウドコンピューティング契約の標準契約条項を策定している。

クラウド・コンピューティング契約の標準契約条項は拘束力を持たないものであり、契約上の必要性に応じて当事者が適応することができる。専門家グループの報告書に基づき、欧州委員会は勧告を採択する。これは 2025 年 9 月 12 日までに行われる予定である。

クラウド・コンピューティング契約の標準契約条項は、切り替えと終了、期間と終了、非分散、非改変、セキュリティと事業継続、および責任に関する要素をカバーする。これらの要素は、第 VI 章でカバーされている側面を反映しているが、第 41 条の目的を達成するために関連するその他の側面も含まれている。41 条は、当事者が公正で合理的、かつ差別のない契約上の権利と義務を伴う契約をドラフトし、交渉するのを支援することを目的としている。

第三国当局による EU 域内の非個人データへの違法なアクセスと移転

56) データ法はデータのローカライゼーションを要求するか？

データ法は、企業が非個人データを国際的に移転する能力を制限するものではない。データ法は、非個人データの自由な流れ規則で提示されている国内データローカライゼーション要件の禁止を変更するものではない。

クラウド・サービスの利用者は、自分の好きなクラウド・プロバイダを選び、どこにデータを保存するかを自由に決めることができる。

57) 第 32 条の目的は何か？

第 32 条は、EU 域内に非個人データを保管することを選択したクラウドサービスプロバイダの顧客が、EU 域外の政府によってそのデータに違法にアクセスされたり、転送されたりすることから保護されることを保証するものである。そのために、クラウドサービスプロバイダは、政府による違法または不法な顧客データへのアクセスや移転を防ぐために、技術的、組織的、法的なあらゆる適切な措置を講じなければならない（第 28 条参照）。

データへの違法なアクセスや移転は、そのようなアクセスや移転が、個人の基本的権利の保護や、企業秘密や知的財産権を含む商業上機密性の高いデータの保護など、EU 法や加盟国の法律に基づく義務に抵触する場合に起こりうる（recital 101 参照）。

顧客の非個人データに対して第三国当局からアクセスまたは転送要求がなされた場合、クラウドサービスプロバイダはその適法性を確認する義務がある。例えば、相互法的支援条約などの国際協定に基づく要求の場合、合法性が存在する。国際協定がない場合、要請は、要請の比例性や司法審査など、EU 法秩序の基本的な規則や規範に沿った一定の手続き上のセーフガードに従わなければならない。

特定の団体がそのカテゴリーに入るかどうかを評価する際、「政府」や「公的機関」の定義が狭すぎてはならない。

58) 第 32 条は、企業間あるいは企業内部での国際的なデータ移転に適用されるか？

データガバナンス法の第 31 条と同様に、データ法の第 32 条は国際的なデータフローのごく一部、つまり EU 域外の公的機関による非個人データへの違法なアクセスや移転に起因するもののみを対象としている。

これらの条文は、EU 国境の両側の民間事業体間のデータ移転は対象としていない。むしろ、EU または加盟国の法律に反する EU 域外の公的機関による非個人データへのアクセスや移転を防止するものである。個人データの国際的な移転は GDPR の下で規制されている。

59) データ処理サービスプロバイダーは、政府による違法なデータへのアクセスやデータ移転を防ぐために、どのような対策を講じるべきか？

その中には、データの暗号化、頻繁な監査の実施、関連するセキュリティ保証認証制度の検証された遵守、企業ポリシーの変更などが含まれる。欧州委員会は、このような対策の開発、配備、定期的な更新を奨励している。

欧州委員会は今後、EDIB の助言に従い、この点について所轄官庁にさらなる指針を示すことを決定する可能性がある。

60）データ処理サービスプロバイダは、第三国当局からの要請を受けてデータへのアクセスまたはデータ転送を許可するかどうかを決定する前に、どの団体に相談することができるか？

データ法第 VII 章に基づく「法的事項の国際協力に権限を有する関連国内機関または当局」を特定するために、データ処理サービスプロバイダは、加盟国のどの事業体が通常相互法的援助条約（MLAT）の履行を担当しているかを確認しなければならない。フランスの場合、例えばフランス司法省の一部門である Bureau de l'entraide pénalee internationale が該当する。ドイツでは、連邦司法局が国際協力の中心的な役割を担っている。

疑義がある場合、受取人は加盟国のデータ・コーディネーターに相談することもできる。

相互運用性

61） 欧州委員会は、標準の代わりに共通の仕様を課すことができるか？

データ法は、共通仕様を押し付けるのではなく、EU の標準化団体によって標準が開発されることを明確に希望している。共通仕様は、本規則の必須要件への準拠を促進するための例外的な予備的解決策としてのみ採用されるべきであり、標準化プロセスが阻害されている場合、または適切な調和された標準の確立が遅れている場合にのみ採用されるべきである。

さらに、欧州委員会は、欧州データ革新委員会の助言を考慮し、第 33 条 1 項に規定されている必須要件のうち、EU 法によってさらに規定されなければ意図した効果が得られないものをさらに規定する委任法を採択することによって、データ法を補足することができる。

データ処理サービスの相互運用性（第 35 条）のために、データ法は中央連合標準リポジトリを設立する。整合標準と共通仕様の両方への参照をリポジトリで公開することができる。共通仕様は、第 35 条(1)および(2)に規定された要件に適合していれば、オープンな相互運用性仕様に基づいて採用することができる。第 30 条 1 項に従い、Infrastructure as a Service デリバリーモデル以外のデータ処理サービスのプロバイダは、リポジトリで参照される共通仕様および整合規格との互換性を、リポジトリでの公表から少なくとも 12 ヵ月後に確保しなければならない。質問 54 を参照のこと。

62） 欧州委員会は、既存の（例えばセクター別の）標準に取って代わることを意図しているか？

そのような意図はない。その代わり、データ法では、分野別の仕様はその分野特有のニーズに基づいてのみ策定されるべきであり、それは慎重に評価されるべきである。さらに、データ法は、欧州共通のデータ空間の開発など、より具体的な EU 規則を妨げるものであってはならない。

63） 第 36 条の必須要件は国内契約法に影響するか？

スマートコントラクトに適用される必須要件は、国内の契約法には影響しない。スマートコントラクト」の定義から、データ法によって規制されるのは、契約の実行に使用されるコンピュータープログラムだけであり、契約そのものではないことが明らかである。

施行

64）加盟国はデータ法の強制力を確保するためにどのような団体を設置すべきか？

加盟国はデータ法の施行に対処し、第 37 条 5 項に列挙された任務を遂行するために、少なくとも 1 つの管轄当局を指定することが義務付けられている。管轄機関は新設されることもあるが、すでに存在する公的機関の場合もある。加盟国がこのような主務官庁を複数認可する可能性もある。その場合、加盟国はその中から「データ・コーディネーター」を指名しなければならない。「データ・コーディネーター」の役割は、管轄当局間の協力を促進し、データ法に基づく権利の行使を希望する事業体を支援することである（「単一の窓口」として）。実際には、データ・コーディネーターは企業や消費者からの質問を受け、その具体的なケースにおいて適切な「管轄当局」となる認可機関を案内することが期待される。

DPA は、個人データ保護に関する限り、データ法の適用を監視する責任を負っていることに留意することが重要である。

さらに、データ法がすべての分野で効率的に適用されることが極めて重要である。したがって、認可当局は、データ法が他の EU 法または国内法と一貫して施行されるよう、各分野の当局と協力しなければならない。

欧州委員会は、欧州データ革新委員会（European Data Innovation Board）を含め、これらの認可当局と緊密に協力し、データ法のシームレスかつ統一的な適用を確保する。この取り組みには、データへのアクセスと利用の規則を効果的に適用するための分野別ガイドラインを発行することも含まれる。

65）データ法に基づく自分の権利が尊重されていないと考える場合、どの公的機関が助けてくれるか？

加盟国が主務官庁を 1 つしか指定していない場合、この主務官庁がデータ法の適用に関するすべての事項を監督することになる。いずれにせよ、各加盟国の管轄当局の名前は、対応する任務と権限とともに、欧州委員会が管理する一般に公開された登録簿に記載される。データ法の適用に関するすべての問題は、加盟国のデータコーディネーターが窓口になるはずである。場合によっては、データコーディネーターが管轄当局間の協力を促進することもある。

自然人および法人は、国境を越えた問題を含め、常居所地、勤務地または認可のある加盟国の関連する管轄当局に苦情を申し立てるべきである。管轄当局は、同じ加盟国内だけでなく、国境を越えて協力し、助け合う義務がある。

66）データ法の施行における欧州委員会の役割は何か？

データ法の施行は主に加盟国当局の責任であるが、欧州委員会はそれを支援する役割を担っている。欧州委員会は、管轄当局間の協力を促進し、執行におけるベストプラクティスと共通のアプローチを促進する専門家グループである欧州データ革新委員会（EDIB）を主催している。加えて、欧州委員会

は、所轄当局に関する情報、罰則に関する各国の法律や措置に関する情報を一般に公開している。市場関係者がデータ法によって導入された権利と義務を遵守するのを支援するため、欧州委員会は、データ法の規定を反映したデータ共有契約のモデル契約条項およびクラウド・コンピューティング契約の標準契約条項も勧告する予定である。

67) 罰則は EU 全体で統一されているか？

加盟国は、罰則およびその適用に関連するすべての必要な措置を設定する責任を負う。しかし、EU 全体で高い一貫性を確保するため、EDIB はデータ法違反に対する罰則の設定について評価、調整、勧告を採択するプラットフォームとして利用される。

DPA は、その権限の範囲内で、データ法第 II 章、第 III 章および第 V 章に規定された義務の違反に対して GDPR に従って制裁金を課すことができる。EDPS は、その権限の範囲内で、第 V 章に規定された義務の違反に対して、規則（EU）2018/1725 に従って行政制裁金を課すことができる。

68) 法定代表者はいつ指定されるべきか？EU 域外の企業がデータ法を遵守しなかった場合、そのような法定代表者は責任を負うか？

法定代理人の役割は、EU 市場でサービスや製品を提供しているが、EU 域外に設立されている事業体によるデータ法の遵守を促進することである。このような事業体はすべて、EU を拠点とする代表者を指名しなければならない。管轄当局は、EU 域外の事業体の代わりに、または EU 域外の事業体に加えて、データ法の実施に関連するすべての事項について、このような代表者に対応することができる。ただし、その責任はデータ法に基づく代表者としての義務に限定される。データ法における法定代理人の役割と責任は、GDPR における法定代理人の役割と責任に類似している（欧州データ保護委員会ガイドライン 3/2018 参照）。

次のステップと将来の行動

69) 欧州委員会は妥当な報酬に関する指針をいつ発表するか？

データ法第 9 条 5 項に基づき、EDIB はデータ利用可能にするための合理的な補償の算定に関するガイドラインについて、その採択前に諮問を受けなければならない。EDIB は、データ法が適用された後でなければ、この問題について発表する権限を持たない。

70) 相互運用性に関する次のステップは何か？

データ空間における相互運用性に関する要求事項に関するデータ法第 33 条を支持し、欧州委員会は「欧州信頼データフレームワーク」と呼ばれる標準化要求を作成した。

この要請は、欧州標準化ハイレベルフォーラムのデータ相互運用性ワークストリームの勧告に密接に沿った 5 つの EU 標準／標準化成果物を対象としている。

この要請は現在、欧州の標準化団体（CEN、CENELEC、ETSI）、標準化における消費者、環境、労働組合、中小企業を代表する EU の利害関係者団体（SBS、ETUC、ANEC、ECOS）、欧州データ革新委員会と協議中である。

この要請は 2024 年末までに正式に採択される見込みだ。

71) データ共有に関するモデル契約条項とクラウド・コンピューティング契約の標準契約条項の現状はどうなっているか？

データ法第 41 条に基づき、JUST 総局と CNECT 総局が共同で運営する「B2B データ共有とクラウドコンピューティング契約に関する専門家グループ」は現在、データ共有のモデル契約条項とクラウドコンピューティング契約の標準契約条項を策定している。

データ共有に関するモデル契約条項は、データ保有者と利用者、データ保有者とデータ取得者、利用者とデータ取得者間の契約をカバーする。

クラウド・コンピューティング契約の標準契約条項は、切り替えと終了、期間と終了、非分散、非改変、セキュリティと事業継続、および責任に関する要素をカバーする。これらの要素は、第 VI 章でカバーされている側面を反映しているが、第 41 条の目的を達成するために関連するその他の側面も含まれている。41 条は、当事者が公正で合理的、かつ差別のない契約上の権利と義務を伴う契約をドラフトし、交渉するのを支援することを目的としている。

この契約は拘束力を持たず、契約上の必要性に応じて当事者が変更することができる。専門家グループの報告書に基づき、欧州委員会は 2025 年 9 月 12 日までに勧告を採択する予定である。

データ法 FAQ バージョン履歴

バージョン	日付	備考
1.0	06/09/2024	発行
1.1	13/09/2024	ウェブアクセシビリティの改善と「バージョン履歴」セクションの追加