仮日本語訳

Guidelines on the right to data portability
データポータビリティの権利に関するガイドライン

本書面は、ARTICLE 29 DATA PROTECTION WORKING PARTY （第29条作業部会）により2016年12月13日に採択後、修正のうえ2017年4月5日に採択された、“Guidelines on the right to data portability”の英語版の一部を個人情報保護委員会が翻訳したものである。本書面は参考のための仮日本語訳であって、その利用について当委員会は責任を負わないものとし、正確な内容については原文を参照されたい。

TABLE OF CONTENTS

目次

Executive summary

エグゼクティブ・サマリー

Article 20 of the GDPR creates a new right to data portability, which is closely related to the right of access but differs from it in many ways. It allows for data subjects to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller. The purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.

GDPR 第 20 条では、新たにデータポータビリティの権利を規定している。これは、アクセス権と密接に関連しているものの多くの点でそれとは異なる規定である。同条は、構造化され、一般的に利用され機械可読性のある形式で管理者に提供された個人データについてデータ主体が受け取り、さらに別のデータ管理者に移行することを認めている。この新たな権利の目的は、データ主体に権利を付与し、データ主体が自己の個人データをよりコントロールできるようにすることである。

Since it allows the direct transmission of personal data from one data controller to another, the right to data portability is also an important tool that will support the free flow of personal data in the EU and foster competition between controllers. It will facilitate switching between different service providers, and will therefore foster the development of new services in the context of the digital single market strategy.

GDPR 第 20 条では、個人データの、あるデータ管理者から別のデータ管理者への直接の移行が認められているため、データポータビリティの権利は、EU 域内での個人データの自由な流通を支援し管理者間の競争を促進する重要なツールでもある。データポータビリティの権利は、複数の役務提供事業者間での切り替えを促し、これにより、デジタル単一市場戦略の文脈において新たなサービス事業の発展を促進する。

This opinion provides guidance on the way to interpret and implement the right to data portability as introduced by the GDPR. It aims at discussing the right to data portability and its scope. It clarifies the conditions under which this new right applies taking into account the legal basis of the data processing (either the data subject's consent or the necessity to perform a contract) and the fact that this right is limited to personal data provided by the data subject. The opinion also provides concrete examples and criteria to explain the circumstances in which this right applies. In this regard, WP29 considers that the right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity. This new right cannot be undermined and limited to the personal information directly communicated by the data subject, for example, on an online form.

本ガイドラインでは、GDPR で規定されるデータポータビリティの権利の解釈及び実施に関する指針を提供しており、データポータビリティの権利とその範囲の説明を意図している。ここで明示されるのは、この新たな権利がデータ取扱い（データ主体による同意又は契約締結の必要性の何れか）の法的根拠を考慮し適用される場合の条件、及び、この権利がデータ主体が提供した個人データに限定されるということである。 本ガイドラインではまた、この権利が適用される状況を説明するために具体的な事例及び基準が示されている。この点に関し、WP29 は、データポータビリティの権利には、データ主体が認識しつつかつ主体的に提供したデータ及びそのデータ主体が生成した個人データを対象にすると考えている。この新たな権利は損なわれてはならず、またデータ主体が例えばオンラインフォームなどで直接通信した個人情報に限定されない。

As a good practice, data controllers should start developing the means that will contribute to answer data portability requests, such as download tools and Application Programming Interfaces. They should guarantee that personal data are transmitted in a structured, commonly used and machine-readable format, and they should be encouraged to ensure the interoperability of the data format provided in the exercise of a data portability request.
望ましい慣行として、データ管理者は、ダウンロードツールやアプリケーション・プログラミング・インターフェース（API）など、データポータビリティに関する要求に対応できる手段の開発を開始すべきである。データ管理者は、構造化され、一般的に利用され、機械可読性のある形式での個人データの移行を担保し、また、データポータビリティの要求への対応において提供されるデータフォーマットについて相互運用性を担保するべきである。

The opinion also helps data controllers to clearly understand their respective obligations and recommends best practices and tools that support compliance with the right to data portability. Finally, the opinion recommends that industry stakeholders and trade associations work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.
本ガイドラインはまた、データ管理者がそれぞれの義務を明確に理解する助けとなり、さらに、データ管理者がデータポータビリティの権利を遵守できるよう支援するベストプラクティス及びツールも提言する。最後に、本ガイドラインは、データの遂行を目的として、産業界関係者及び事業者団体が協力してポータビリティの権利の要求の実施について統一の相互運用基準及びフォーマットを策定するよう提言する。

I. Introduction
I. 序

Article 20 of the General Data Protection Regulation (GDPR) introduces a new right of data portability. This right allows for data subjects to receive the personal data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance. This right, which applies subject to certain conditions, supports user choice, user control and user empowerment.
一般データ保護規則（以下「GDPR」）第 20 条は、新たにデータポータビリティの権利を規定している。この権利では、データ主体が、管理者に提供した個人データについて、構造化され、一般的に利用され、かつ機械可読性のある形式で受け取り、また、妨害なくそのデータを別のデータ管理者に移行することを認めている。この権利は、特定の条件において適用されるが、これはユーザーによる選択、ユーザーによるコントロール、及びユーザーに権限を持たせることを支えるものである。

Individuals making use of their right of access under the Data Protection Directive 95/46/EC were constrained by the format chosen by the data controller when providing the requested information. **The new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another** (whether to their own systems, the systems of trusted third parties or those of new data controllers).
個人が、データ保護指令（Data Protection Directive）95/46/EC に基づくアクセス権を行使する場合、要求した情報の提供の際にデータ管理者が選択した形式によって制約されていた。**新たなデータポータビリティの権利は、データ主体に自己の個人データについての権限を持たせることを目的としており、これにより、データ主体が、**（データ主体自身のシステムへであれ、委託第三者のシステムへであれ、あるいは新しいデータ管理者のシステムへであれ、）**個人データをある IT 環境から別の IT 環境へ移動、複製又は移行することができることを促進する。**

By affirming individuals' personal rights and control over the personal data concerning them, data portability also represents an opportunity to "re-balance" the relationship between data subjects and data controllers[1].
データポータビリティは、また、各個人の自己の個人データに関する権利及びコントロールを認めることにより、データ主体とデータ管理者との関係について「再びバランスを取る」("re-balance") 機会を表している[1]。

[1] The primary aim of data portability is enhancing individual's control over their personal data and making sure they

Whilst the right to personal data portability may also enhance competition between services (by facilitating service switching), the GDPR is regulating personal data and not competition. In particular, article 20 does not limit portable data to those which are necessary or useful for switching services[2].
データポータビリティに関する権利は、また、サービス間の競争を（サービスの切替を促進することにより）高めうる一方で、GDPRは個人データについては規制しているものの競争については規制していない。特に、第20条は、ポータビリティの対象となるデータをサービスの切替に必要な又は有用なデータに限っているわけではない[2]。

Although data portability is a new right, other types of portability already exist or are being discussed in other areas of legislation (e.g. in the contexts of contract termination, communication services roaming and trans-border access to services[3]). Some synergies and even benefits to individuals may emerge between the different types of portability if they are provided in a combined approach, even though analogies should be treated cautiously.
データポータビリティの権利は新しい権利であるものの、他の種類のポータビリティは、他の法分野（例えば、契約終了時の文脈、通信サービスのローミングや各種サービスに対する越境アクセス[3]）で既に存在しているか又は現在検討されている。異なるタイプのポータビリティについて、類似性については注意して扱われる必要があるが、組合せた方法で提供されれば、異なるタイプのポータビリティの間で何らかの相乗効果や、個人の利益すら生じるかもしれない。

This Opinion provides guidance to data controllers so that they can update their practices, processes and policies, and clarifies the meaning of data portability in order to enable data subjects to efficiently use their new right.
本ガイドラインは、データ管理者がその慣行、取扱い及び方針をアップデートすることを可能にするためのデータ管理者向けの指針を提供するものである。また、本ガイドラインでは、データ主体が効率的に自己の新たな権利を行使することができるよう、データポータビリティの意味を明確化している。

play an active role in the data ecosystem.
データポータビリティの主な目的は、個人の自らについての個人データについてのコントロールを高め、個人がデータのエコシステムの中で積極的な役割を担うことを確保することにある。

[2] For example, this right may allow banks to provide additional services, under the user's control, using personal data initially collected as part of an energy supply service.
例えば、この権利は、銀行が、ユーザーのコントロールのもとで、当初エネルギー供給サービスの一部として収集した個人データを使用する追加のサービスを提供することを可能にしうる。

[3] See European Commission agenda for a digital single market: https://ec.europa.eu/digital-agenda/en/digital-single-marketsingle-market, in particular, the first policy pillar "Better online access to digital goods and services".

II. What are the main elements of data portability?
II. データポータビリティの主な要素は何か？

The GDPR defines the right of data portability in Article 20 (1) as follows:
GDPR では、第 20 条(1)においてデータポータビリティの権利を以下のように定義している。

> *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided [...]*
> *データ主体は、当該データ主体が管理者に提供した当該データ主体に関する個人データについて、構造化され、一般的に利用され、機械可読性のある形式で受け取る権利があり、当該データを、個人データが提供された管理者の妨害なしに、他の管理者に移行する権利がある。（略）*

- **A right to receive personal data**
- **個人データを受領する権利**

Firstly, data portability is a **right of the data subject to receive a subset of the personal data** processed by a data controller concerning him or her, and to store those data for further personal use. Such storage can be on a private device or on a private cloud, without necessarily transmitting the data to another data controller.
最初に、データポータビリティとは、データ管理者がデータ主体に関して取扱った**個人データのサブセットをデータ主体が受け取る権利であり**、また、更なる個人的な使用のためにこれらのデータを保管する権利である。その保管は、そのデータを必ずしも別のデータ管理者に移行することなく、私的な機器又は私的なクラウドで行うことができる。

In this regard, data portability complements the right of access. One specificity of data portability lies in the fact that it offers an easy way for data subjects to manage and reuse personal data themselves. These data should be received "in a structured, commonly used and machine readable format". For example, a data subject might be interested in retrieving his current playlist (or a history of listened tracks) from a music streaming service, to find out how many times he listened to specific tracks, or to check which music he wants to purchase or listen to on another platform. Similarly, he may also want to retrieve his contact list from his webmail application, for example, to build a wedding list, or get information about purchases using different loyalty cards, or to assess his or her carbon footprint[4].
この点において、データポータビリティはアクセス権を補完する。データポータビリティの

特異性は、データ主体が自己の個人データを容易に管理し再利用できるようにしている点にある。こうしたデータは「構造化され、一般的に利用される、機械可読性のある形式」で受け取られるべきである。例えば、あるデータ主体は、特定の楽曲を何度聞いたか確認するため、又は別のプラットフォームでどの楽曲を購入又は聴きたいかを決めるため、音楽配信サービスから自分の最新のプレイリスト（又は楽曲を聴いた履歴）を取り戻すことに関心を持つかもしれない。同様に、このデータ主体は、また、利用しているウェブメールアプリケーションから自分の連絡先リストを取り戻し、例えば、結婚式の招待客リストを作成したり、異なる会員カードでの購買記録を入手したり、自分の二酸化炭素排出量の情報を算定したいと考えるかもしれない[4]。

- **A right to transmit personal data from one data controller to another data controller**
- **あるデータ管理者から別のデータ管理者へ個人データを移行する権利**

Secondly, Article 20(1) provides data subjects with the **right to transmit personal data from one data controller to another data controller** "without hindrance". Data can also be transmitted directly from one data controller to another on request of the data subject and where it is technically feasible (Article 20(2)). In this respect, recital 68 encourages data controllers to develop interoperable formats that enable data portability[5] but without creating an obligation for controllers to adopt or maintain processing systems which are technically compatible[6]. The GDPR does, however, prohibit controllers from establishing barriers to the transmission.

次に、第 20 条(1)では、「妨害なしに」**個人データをあるデータ管理者から別のデータ管理者へ移行する権利**をデータ主体に付与している。データは、データ主体からの要請があり、それが技術的に実行可能である場合には、直接的に管理者から別のデータ管理者に移行することができる（第 20 条（2））。この点において、前文第 68 項は、データ管理者に対し、データポータビリティを可能にする[5]、当該フォーマットと管理者に技術的に互換性のある取扱システムの導入又は維持の義務を負わせず、相互運用可能なフォーマットを開発する

[4] In these cases, the processing performed on the data by the data subject can either fall within the scope of household activities, when all the processing is performed under the sole control of the data subject, or it can be handled by another party, on the data subject's behalf. In the latter case, the other party should be considered as data controller, even for the sole purpose of personal data storage, and must comply with the principles and obligations laid down in the GDPR.
こうした場合、データ主体が行ったデータ取扱いは、全てのデータ取扱いがデータ主体のみのコントロールのもとで行われた場合に家庭での活動(household activity)の範囲に該当しうるか、又は、データ主体に代わって他者によって取り扱われうる。後者の場合、当該他者は、個人データの保管のみの目的であったとしても、データ管理者として捉えられるべきであり、GDPR に定められた原則及び義務を遵守しなければならない。

[5] See also section V.
セクション V.参照

[6] As a consequence, special attention should be paid to the format of the transmitted data, so as to guarantee that the data can be re-used, with little effort, by the data subject or another data controller. See also section V.
結果として、移行データの形式については、当該データがデータ主体又は他のデータ管理者によって少ない労力で再利用できるよう、特別の注意が払われるべきである。セクション V.も参照。

ことを推奨している[6]。しかしながら、GDPR は、管理者が移行に障害を設けることを禁じている。

In essence, this element of data portability provides the ability for data subjects not just to obtain and reuse, but also to transmit the data they have provided to another service provider (either within the same business sector or in a different one). In addition to providing consumer empowerment by preventing "lock-in", the right to data portability is expected to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner, under the data subject's control[7]. Data portability can promote the controlled and limited sharing by users of personal data between organisations and thus enrich services and customer experiences[8]. Data portability may facilitate transmission and reuse of personal data concerning users among the various services they are interested in.
つまり、データポータビリティのこの要素では、データ主体に対し、自己の個人データを受け取り再利用する権利のみならず、提供した個人データを別の（同一のビジネスセクター又は異なるビジネスセクターの）サービスプロバイダーに移行する権利も規定されている。データポータビリティの権利により、消費者の「囲い込み」防止による消費者への権限付与に加え、イノベーション創出の機会及びデータ主体によるコントロール下におけるデータ管理者間での安全かつ安心な個人データ共有の機会の促進も見込まれる[7]。データポータビリティは、組織間でのユーザーによりコントロールおよび制限された個人データの共有を促進し、ひいては、サービス及びユーザー体験の向上の促進も可能となる[8]。データポータビリティでは、ユーザーが関心のある様々なサービス間で、ユーザーに関する個人データの移行及び再利用を促進しうる。

- **Controllership**
- **管理者の地位**

Data portability guarantees the right to receive personal data and to process them, according to the data subject's wishes[9].

[7] See several experimental applications in Europe, for example MiData in the United Kingdom, MesInfos / SelfData by FING in France.
例えば、英国の MiData、フランスの FING による MesInfos / SelfData など、ヨーロッパにおけるいくつかの試験的な適用を参照。
[8] The so-called quantified self and IoT industries have shown the benefit (and risks) of linking personal data from different aspects of an individual's life such as fitness, activity and calorie intake to deliver a more complete picture of an individual's life in a single file.
いわゆる自己定量化（quantified self）及び IoT 産業は、個人の生活について異なる観点から得た健康状態、活動、カロリー摂取量などの個人データを関連付け、個人の生活のより完全な全体像を 1 つのファイルにまとめることの利益（及びリスク）を示している。
[9] The right to data portability is not limited to personal data that are useful and relevant for similar services provided by competitors of the data controller.
データポータビリティの権利にかかる個人データは、データ管理者の競合他社により提供される類似のサ

データポータビリティは、データ主体の要望により、個人データを受け取り、そしてそれを取扱う権利を保証する[9]。

Data controllers answering data portability requests, under the conditions set forth in Article 20, are not responsible for the processing handled by the data subject or by another company receiving personal data. They act on behalf of the data subject, including when the personal data are directly transmitted to another data controller. In this respect, the data controller is not responsible for compliance of the receiving data controller with data protection law, considering that it is not the sending data controller that chooses the recipient. At the same time the controller should set safeguards to ensure they genuinely act on the data subject's behalf. For example, they can establish procedures to ensure that the type of personal data transmitted are indeed those that the data subject wants to transmit. This could be done by obtaining confirmation from the data subject either before transmission or earlier on when the original consent for processing is given or the contract is finalised.
第 20 条の規定に基づくデータポータビリティの要求に対応するデータ管理者は、データ主体によるデータ取扱い又は個人データを受領した別の会社によるデータ取扱いには責任を負わない。データ管理者は、その個人データが直接他のデータ管理者に移行される場合を含め、データ主体のために行動する。この点において、移行元のデータ管理者は、データの移行先を選択するのは移行元のデータ管理者ではないことに鑑み、移行先のデータ管理者のデータ保護法の遵守につき責任を負わない。同時に、データ管理者は、自己が真にデータ主体のために行動することを確保するための保護措置を講じるべきである。例えば、データ管理者は、移行された個人データの種類が真にデータ主体が移行したいと望むデータであることを確保するための手続を設けることができる。これは、移行前に又は取扱いについて最初の同意が与えられた時点若しくは契約が確定した時点の早い時期に、データ主体から確認を得ることによってなしうる。

Data controllers answering a data portability request have no specific obligation to check and verify the quality of the data before transmitting it. Of course, these data should already be accurate, and up to date, according to the principles stated in Art 5(1) of the GDPR. Moreover, data portability does not impose an obligation on the data controller to retain personal data for longer than is necessary or beyond any specified retention period[10]. Importantly, there is no additional requirement to retain data beyond the otherwise applicable retention periods, simply to serve any potential future data portability request.
データポータビリティの要求に対応するデータ管理者には、データを移行する前にその質をチェックし確かめる特定の義務はない。もちろん、これらのデータは、GDPR 第 5 条(1)に定められている原則に従い、既に正確なものであり、最新のものであるべきである。さらに、

ービスに有用であり関連する個人データに限られない。

データポータビリティでは、データ管理者に対し、個人データの保管について必要な期間又は特定の保管期間を超える期間保管する義務は課していない[10]。重要なのは、データ管理者に対し、単に将来のデータポータビリティの要求に対応するためだけに、別途適用されることとなる保管期間を超えてデータを保管するという追加要件はないということである。

Where the personal data requested are processed by a data processor, the contract concluded in accordance with Article 28 of the GDPR must include the obligation to assist "the controller by appropriate technical and organisational measures, (…) to respond to requests for exercising the data subject's rights". The data controller should therefore implement specific procedures in cooperation with its data processors to answer data portability requests. In case of a joint controllership, a contract should allocate clearly the responsibilities between each data controller regarding the processing of data portability requests.
要求された個人データがデータ処理者によって取扱われる場合、GDPR 第 28 条に従い締結された契約には、「(…) 管理者がデータ主体の権利行使の要求に応じる義務を履行するため、適切な技術的及び組織的対策によって」支援する義務が含まれていなければならない。したがって、データ管理者は、データポータビリティの要求に対応するため、データ処理者と協力して特定の手続を実行すべきである。共同管理者の場合には、契約では、データポータビリティの要求に関する各データ管理者間の責任を明確に割当てるべきである。

In addition, a receiving data controller[11] is responsible for ensuring that the portable data provided are relevant and not excessive with regard to the new data processing. For example, in the case of a data portability request made to a webmail service, where the request is used by the data subject to obtain emails and send them to a secured archive platform, the new data controller does not need to process the contact details of the data subject's correspondents. If this information is not relevant with regard to the purpose of the new processing, it should not be kept and processed. In any case, receiving data controllers are not obliged to accept and process personal data transmitted following a data portability request. Similarly, where a data subject requests the transmission of details of his or her bank transactions to a service that assists in managing his or her budget, the receiving data controller does not need to accept all the data, or to retain all the details of the transactions once they have been labelled for the purposes of the new service. In other words, the data accepted and retained should only be that which is necessary and relevant to the service being provided by the receiving data controller.

[10] In the example above, if the data controller does not retain a record of songs played by a user then this personal data cannot be included within a data portability request.
前述の例において、データ管理者がユーザーの再生した楽曲の記録を保管していない場合、この個人データはデータポータビリティの要求の範囲に包含されない。

また、個人データを受領したデータ管理者[11]は、提供されたデータポータビリティの対象となるデータ（ポータブルデータ）が、新たなデータ取扱いに関して関連性があり、過度でないことを担保する責任を有する。例えば、ウェブメールサービスへのデータポータビリティの要求の場合で、データ主体が電子メールを取得し、その電子メールを安全が確保されているアーカイブプラットフォームに送信するために利用するとき、新たなデータ管理者は、そのデータ主体のメールの送信先の記録を取扱うべきではない。この情報が新たなデータ取扱いの目的に関連しない場合、その情報を保管し取扱う必要はない。いずれにしても、データを受領する管理者には、データポータビリティの要求により移行された個人データを受領し取扱う義務はない。同様に、データ主体の銀行取引の詳細について、データ主体の家計管理を支援しているサービス事業者に対し、その詳細を移行したい旨の要求がデータ主体からあった場合、データを受領する管理者は、その新たなサービスのためにその銀行取引の詳細が分類処理されていれば、すべてのデータを受領し又はすべてのデータについて保管する必要はない。つまり、受け入れ、保有するデータは、受領するデータ管理者が提供するサービスに必要かつ関連するもののみに限られるべきである。

A “receiving” organization becomes a new data controller regarding these personal data and must respect the principles stated in Article 5 of the GDPR. Therefore, the ”new” receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data in accordance with the transparency requirements set out in Article 14[12]. As for any other data processing performed under its responsibility, the data controller should apply the principles laid down in Article 5, such as lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, integrity and confidentiality, storage limitation and accountability[13].
データを「受領」した機関は、個人データの新たなデータ管理者となり、GDPR 第 5 条に規定される原則を遵守しなければならない。よって、「新たな」データを受領した管理者は、データ主体に対し、第 14 条に規定されている透明性の要件に従い、ポータブルデータの移行の要求に先立って新たな取扱いの目的を明示し直接伝達しなければならない[12]。データ管理者がその責任の下で行う他の取扱いについては、管理者は、第 5 条に定められている原則、例えば、適法性、公正性及び透明性、目的の限定、データ最小化、正確性、完全性及び

[11] i.e. that receives personal data following a data portability request made by the data subject to another data controller.
すなわち、データ主体による別のデータ管理者へのデータポータビリティの要求によって、個人データを取得した者。

[12] In addition, the new data controller should not process personal data, which are not relevant, and the processing must be limited to what is necessary for the new purposes, even if the personal data are part of a more global data-set transmitted through a portability process. Personal data, which are not necessary to achieve the purpose of the new processing, should be deleted as soon as possible.
さらに、新たなデータ管理者は、関連性のない個人データを取扱うべきではなく、その個人データが、データポータビリティのプロセスを通じて移行されるグローバルデータセットの一部であったとしても、データ取扱いは新たな目的に必要とされるものに制限されなければならない。新たな取扱いの目的の達成に必要でない個人データは、可能な限り速やかに削除されるべきである。

機密性、保管の制限及びアカウンタビリティを適用すべきである[13]。

Data controllers holding personal data should be prepared to facilitate their data subject's right to data portability. Data controllers can also choose to accept data from a data subject, but are not obliged to.
個人データを保有するデータ管理者は、そのデータ主体のデータポータビリティの権利を促進するための準備をするべきである。データ管理者は、データ主体からデータを受領することも選択できるが、これは義務付けられてはいない。

- **Data portability vs. other rights of data subjects**
- **データポータビリティとその他のデータ主体の権利との比較**

When an individual exercises his or her right to data portability he or she does so without prejudice to any other right (as is the case with any other rights in the GDPR). A data subject can continue to use and benefit from the data controller's service even after a data portability operation. Data portability does not automatically trigger the erasure of the data[14] from the systems of the data controller, and does not affect the original retention period applying to the data which have been transmitted. The data subject can exercise his or her rights as long as the data controller is still processing the data. Equally, if the data subject wants to exercise his or her right to erasure ("right to be forgotten" under Article 17), data portability cannot be used by a data controller as a way of delaying or refusing such erasure.
個人がデータポータビリティの権利を行使する際、その個人は、(GDPRにおける他の権利の場合と同様に）その他の権利を損なうことなくこれを行使することができる。データ主体は、データポータビリティの実施後でも、データ管理者のサービスを引き続き利用し利益を得ることができる。データポータビリティが要因となって、データ管理者のシステムからデータが自動的に削除されるということはなく[14]、データポータビリティは、移行されるデータに適用される元来の保管期間にも影響を与えない。データ主体は、データ管理者が当該データを取扱う限り、依然として自己の権利を行使することができる。同様に、データ主体が自己の権利を行使しデータの削除（第17条の「忘れられる権利」）を希望する場合、データポータビリティの権利行使は、データ管理者において、その削除の遅延又は拒否などの方法に使われてはならない。

[13] Once received by the data controller, the personal data sent as part of the right to data portability can be considered as "provided by" the data subject and be re-transmitted according to the right to data portability, to the extent that the other conditions applicable to this right (ie. the legal basis of the processing, …) are met.
データ管理者によっていったん取得されると、データポータビリティの権利の一部として送られた個人データは、データ主体「によって提供された」と捉えることが可能で、また、データポータビリティの権利によって、当該権利の他の条件（すなわち、取扱いの適法性など。）が満たされる範囲で、再び移行することが可能である。
[14] as stated in Article 17 of the GDPR

Should a data subject discover that personal data requested under the right to data portability does not fully address his or her request, any further request for personal data under a right of access should be fully complied with, in accordance with Article 15 of the GDPR.
データ主体が、データポータビリティの権利に基づき要求される個人データでは自己の要求が十分には対応されないと考える場合、アクセス権に基づく更なる個人データの要求について、GDPR 第 15 条を遵守しなければならない。

Furthermore, where a specific European or Member State law in another field also provides for some form of portability of the data concerned, the conditions laid down in these specific laws must also be taken into account when satisfying a data portability request under the GDPR. First, if it is clear from the request made by the data subject that his or her intention is not to exercise rights under the GDPR, but rather, to exercise rights under sectorial legislation only, then the GDPR's data portability provisions will not apply to this request[15]. If, on the other hand, the request is aimed at portability under the GDPR, the existence of such specific legislation does not override the general application of the data portability principle to any data controller, as provided by the GDPR. Instead, it must be assessed, on a case by case basis, how, if at all, such specific legislation may affect the right to data portability.
さらに、他の分野での特定の EU 法又は加盟国の国内法も関連するデータのポータビリティの形式について規定している場合には、GDPR に従ってデータポータビリティの要求に対応する際に、これらの特定の法律も考慮されなければならない。まず、データ主体による要求から、データ主体が GDPR に基づく権利を行使するのではなく他分野の法律のみに基づき権利を行使する意図が明らかである場合には、GDPR のデータポータビリティの規定はこの要求には適用されない[15]。一方、仮にその要求が GDPR のポータビリティを求めるものである場合、GDPR が規定するように、そのような特定の法律の存在が、すべてのデータ管理者へのデータポータビリティの一般的適用に優先することはない。むしろ、そのような特定の法律が、もしデータポータビリティの権利に影響を与えるならば、どのように影響を与えるかをケース・バイ・ケースで評価しなければならない。

III. When does data portability apply?
III. データポータビリティはいつ適用されるか？

[15] For example, if the data subject's request aims specifically at providing access to his banking account history to an account information service provider, for the purposes stated in the Payment Services Directive 2 (PSD2) such access should be granted according to the provisions of this directive.
例えば、データ主体の要求が、Paymennt Services Directive 2 (PSD2)で規定される目的のために、アカウント情報サービスプロバイダーに自己の銀行口座の取引履歴についてアクセスを与えることを意図としている場合、このようなアクセスは当該 directive によって権限付与されるべきである。

- **Which processing operations are covered by the right to data portability?**
- **どの取扱作業がデータポータビリティの権利の対象となるか？**

Compliance with the GDPR requires data controllers to have a clear legal basis for the processing of personal data.
GDPR は、データ管理者に対し、個人データの取扱いについて明確な法的根拠に基づくことを義務付けている。

In accordance with Article 20(1)(a) of the GDPR, **in order to fall under the scope of data portability**, processing operations must be based:

- either on the data subject's consent (pursuant to Article 6(1)(a), or pursuant to Article 9(2)(a) when it comes to special categories of personal data);
- or, on a contract to which the data subject is a party pursuant to Article 6(1)(b).

GDPR 第 20 条(1)(a）に基づき、**データポータビリティの対象に該当するためには**、取扱作業は、以下のいずれかに基づき実施されなければならない。

- データ主体の同意（第 6 条(1)(a）又は特別な種類の個人データについては第 9 条(2)(a)に従う）、又は、
- 第 6 条(1)(b)に従い、データ主体が当事者である契約。

As an example, the titles of books purchased by an individual from an online bookstore, or the songs listened to via a music streaming service are examples of personal data that are generally within the scope of data portability, because they are processed on the basis of the performance of a contract to which the data subject is a party.
例えば、個人がオンライン書店で購入した書籍のタイトルや音楽配信サービスを通じて聞いた楽曲は、データ主体が当事者である契約の履行に基づき取扱われているため、一般的なデータポータビリティの対象に入る個人データである。

The GDPR does not establish a general right to data portability for cases where the processing of personal data is not based on consent or contract[16]. For example, there is no obligation for financial institutions to answer a data portability request concerning personal data processed as part of their obligations obligation to prevent and detect money laundering and other financial crimes; equally, data portability does not cover professional contact details processed in a business to business relationship in cases where the processing is neither based on the consent of the data subject nor on a contract to which he or she is a party.
GDPR では、個人データの取扱いが同意にも契約にも基づいていない場合については、デー

タポータビリティの一般的権利の対象としていない[16]。例えば、金融機関には、マネーロンダリング及びその他の金融犯罪を防止及び摘発する義務の一環として取扱った個人データに関するデータポータビリティの要求には対応する義務はない。同様に、データポータビリティは、企業間での関係において取扱われた仕事上の連絡先の詳細については、その取扱いがそのデータ主体の同意を得ておらず、また当該データ主体が契約の当事者でもない場合には、認められない。

When it comes to employees' data, the right to data portability typically applies only if the processing is based on a contract to which the data subject is a party. In many cases, consent will not be considered freely given in this context, due to the imbalance of power between the employer and employee[17]. Some HR processings instead are based on the legal ground of legitimate interest, or are necessary for compliance with specific legal obligations in the field of employment. In practice, the right to data portability in an HR context will undoubtedly concern some processing operations (such as pay and compensation services, internal recruitment) but in many other situations a case by case approach will be needed to verify whether all conditions applying to the right to data portability are met.

従業員のデータについては、データポータビリティの権利は、典型的には、そのデータ主体が契約の当事者である場合にのみ認められる。多くの場合、雇用者と従業員間の力が不均衡であるため、この文脈においては、同意が自由に与えられるとは解されない[17]。いくつかの人事処理は、むしろ、正当な利益に係る法的根拠に基づいているか、あるいは、雇用の分野における特定の法的義務の遵守のために必要である。実際には、人事の場合のデータポータビリティの権利は、間違いなくいくつかの取扱いの実行（給与及び報酬に関するサービス、

[16] See recital 68 and Article 20(3) of the GDPR. Article 20(3) and Recital 68 provide that data portability does not apply when the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, or when a data controller is exercising its public duties or complying with a legal obligation. Therefore, there is no obligation for data controllers to provide for portability in these cases. However, it is a good practice to develop processes to automatically answer portability requests, by following the principles governing the right to data portability. An example of this would be a government service providing easy downloading of past personal income tax filings. For data portability as a good practice in case of processing based on the legal ground of necessity for a legitimate interest and for existing voluntary schemes, see pages 47 & 48 of WP29 Opinion 6/2014 on legitimate interests (WP217).
前文第 68 項及び第 20 条(3)を参照。第 20 条(3)及び前文第 68 項では、データ取扱いが、公共の利益のため若しくはデータ管理者に付与された公的権限の執行のため実施される作業の遂行に必要である場合又はデータ管理者が公務を履行又は法的義務を遵守している場合、データポータビリティの権利は適用されないと規定されている。よって、こうした場合は、データ管理者にはデータポータビリティに基づく提供を実施する義務はない。しかしながら、データポータビリティの権利の準拠原則に従い、データポータビリティの要求に対し自動的に対応できるプロセスを作成しておくことは望ましい慣行である。一例として、政府が提供している、これまで納付した個人所得税のデータを容易にダウンロードできるサービスが挙げられる。正当な利益に必要な法的根拠及び現存する自主的なスキームに必要な法的根拠に基づく取扱いにおける望ましい慣行については、WP29 Opinion 6/2014 の 47 頁及び 48 頁「正当な利益」（WP217）を参照のこと。

[17] As the WP29 outlined in its Opinion 8/2001 of 13 September 2001 (WP48).
WP29 が Opinion 8/2001 of 13 September 2001 (WP48)で説明したとおり。

インターン募集など）に関連するが、それ以外の多くの場合、データポータビリティの権利に適用されるすべての条件を満たしているかを確認するためには、ケース・バイ・ケースのアプローチが必要であろう。

Finally, the right to data portability only applies if the data processing is "carried out by automated means", and therefore does not cover most paper files.
最後に、データポータビリティの権利は、データ取扱いが「自動化された手段により実施された」場合にのみ適用される。よって、大部分の紙のファイルはこれに該当しない。

- What personal data must be included?
- どの個人データが含まれなければならないか？

Pursuant to Article 20(1), to be within the scope of the right to data portability, data must be:
- personal data concerning him or her, and
- which he or she has *provided* to a data controller.

第 20 条(1)に従い、データポータビリティの権利の対象となるには、データは以下のものでなくてはならない。
- データ主体に係る個人データ、及び
- データ主体がデータ管理者に*提供した*個人データ

Article 20(4) also states that compliance with this right shall not adversely affect the rights and freedoms of others.
第 20 条(4)では、この権利の遵守により他人の権利及び自由に不利な影響を与えてはならないことが規定されている。

<u>First condition: personal data concerning the data subject</u>
<u>第一の条件：データ主体に関する個人データであること</u>

Only personal data is in scope of a data portability request. Therefore, any data that is anonymous[18] or does not concern the data subject, will not be in scope. However, pseudonymous data that can be clearly linked to a data subject (e.g. by him or her providing the respective identifier, cf. Article 11 (2)) is within the scope.
データポータビリティの要求の対象となるデータは個人データのみである。よって、匿名化データ [18] 又はデータ主体に関連していないデータは全て要求の対象ではない。しかしなが

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

ら、データ主体に明確に関連付けることができる仮名化データ（例えば、データ主体が個々の識別子を提供しているなど。第 11 条(2)参照。）は要求の対象となる。

In many circumstances, data controllers will process information that contains the personal data of several data subjects. Where this is the case, data controllers should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". As an example, telephone, interpersonal messaging or VoIP records may include (in the subscriber's account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests, because the records are (also) concerning the data subject. However, where such records are then transmitted to a new data controller, this new data controller should not process them for any purpose which would adversely affect the rights and freedoms of the third-parties (see below: third condition).
多くの場合、データ管理者は複数名のデータ主体の個人データが含まれる情報を取扱う。こうした場合、データ管理者は、「データ主体に関する個人データ」という文言を過度に限定して解釈すべきでない。例えば、通話記録、個人間のメッセージ交換記録又は IP 電話記録には（契約者のアカウント履歴において）発信及び着信に関連する第三者の詳細な情報が含まれていることがありうる。こうした記録には、複数名の個人データが含まれているものの、それらの記録がデータ主体に（も）関連するため、契約者は、データポータビリティの要求を行うことでこれらの記録を取得できるべきである。しかしながら、こうした記録が新たなデータ管理者に移行される場合、この新たな管理者は、第三者の権利及び自由に不利な影響を与えるような使用目的でこうした記録を取扱ってはならない（後述の「第三の条件」を参照のこと）。

Second condition: data provided by the data subject
第二の条件：データ主体により提供されたデータであること

The second condition narrows the scope to data "provided by" the data subject.
第二の条件では、データの範囲がデータ主体「により提供された」データに狭められている。

There are many examples of personal data, which will be knowingly and actively "provided by" the data subject such as account data (e.g. mailing address, user name, age) submitted via online forms. Nevertheless, data "provided by" the data subject also result from the observation of his activity. As a consequence, the WP29 considers that to give its full value to this new right, "provided by" should also include the personal data that are observed from the activities of users such as raw data

processed by a smart meter or other types of connected objects[19], activity logs, history of website usage or search activities.
認識しつつかつ主体的にデータ主体「により提供された」データとなる個人データの事例は多く、オンラインフォームを通じて提出されたアカウントデータ（メーリングアドレス、ユーザー名、年齢）などが挙げられる。しかしながら、データ主体「によって提供された」データは、また、当該データ主体の活動の観察の結果からも生じるものである。結果として、WP29 は、この新しい権利に完全な価値を与えるためには、「によって提供された」には、例えばスマートメーター又は他の種類の接続物 [19] で取扱われた生データ、行動記録、ウェブサイト利用履歴又は検索履歴など、ユーザーの行動から観察された個人データも含まれるべきである。

This latter category of data does not include data that are created by the data controller (using the data observed or directly provided as input) such as a user profile created by analysis of the raw smart metering data collected.
後者のデータカテゴリには、収集した未加工のスマートメーターデータの分析により作成されたユーザプロファイルなど、データ管理者が（観察により又は直接入力により提供されたデータを使用して）作成したデータは含まれない。

A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":

- **Data actively and knowingly provided by the data subject** (for example, mailing address, user name, age, etc.)
- **Observed data provided by the data subject by virtue of the use of the service or the device.** They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.

データがデータポータビリティの権利の対象に該当するか否かを判断するために、データの出所によりデータを異なる分類に区分することができる。以下の分類項目は「データ主体により提供された」データの対象となりうる。

- **データ主体により主体的にかつ認識しつつ提供されたデータ**（メーリングアドレス、ユーザ名、年齢など）

[19] By being able to retrieve the data resulting from observation of his or her activity, the data subject will also be able to get a better view of the implementation choices made by data controller as to the scope of observed data and will be in a better situation to choose what data he or she is willing to provide to get a similar service, and be aware of the extent to which his or her right to privacy is respected.
自らの行動についての観察の結果生じるデータを取り戻すことができるようにすることによって、データ主体は、データ管理者による観察データの範囲についての実施の選択に、より良く判断することができるようにもなり、また、類似のサービスにおいてどのデータを提供するかについてより良く選択することができるようになり、さらに、自らのプライバシーが尊重されている程度を知ることができる。

- **サービス又は機器を利用することによりデータ主体により提供された観察データ。**こうしたデータには、例えば個人の検索履歴、交通データ、位置データなどが含まれうる。また、身体に装着できる装置などにより把握されている心拍数などのその他の生データも含まれうる。

In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as "provided by" the data subject. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as "provided by the data subject" and thus will not be within scope of this new right[20].

対照的に、推定データや派生データは、「データ主体により提供された」データをもとにデータ管理者が作成したものである。例えば、ユーザーの健康の評価結果やリスクマネジメント及び金融規制（例えば、クレジットスコアの割り当て又はマネーロンダリング防止に関するルールの遵守）において作成されたプロファイルは、それ自体では、データ主体により「提供された」とはみなされない。このようなデータは、データ管理者が保管しているプロファイルに含まれているかもしれず、また、データ主体により（例えばその行為を通じて）提供されたデータの分析から推定され又は派生されたものであるが、こうしたデータは一般的には「データ主体により提供された」データと見なされない。したがって、これらはこの新たな権利の範囲には含まれない[20]。

In general, given the policy objectives of the right to data portability, the term "provided by the data subject "must be interpreted broadly, and should exclude "inferred data" and "derived data", which include personal data that are created by a service provider (for example, algorithmic results). A data controller can exclude those inferred data but should include all other personal data provided by the data subject through technical means provided by the controller[21].

一般的に、データポータビリティ権利の政策目標を考慮すると、「データ主体により提供さ

[20] Nevertheless, the data subject can still use his or her "right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data" as well as information about "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject", according to Article 15 of the GDPR (which refers to the right of access).

それでもなお、データ主体は、やはり、自己の「個人データについて取扱っているか否かをデータ管理者に確認し、取扱っている場合、個人データにアクセスする権利」を行使でき、「第 22 条(1)及び(4)に規定されている、プロファイリングを含めた自動化された意思決定の有無に関する情報であって、少なくともGDPR 第 15 条（アクセス権の規定）に規定されている、関連する論理及びデータ主体に関する取扱いについて重要かつ想定される結果に関する有意義な情報」を利用できる。

れた」という文言は、広義に解釈されなければならず、また、サービスプロバイダーが作成した個人データ（例えば、アルゴリズムによる結果。）を含む、「推定データ」と「派生データ」は除外すべきである。データ管理者は、これら推定データを除外できるが、データ主体が管理者の提供する技術的手段を通じてデータ管理者に提供したその他の全ての個人データについては範囲に含むべきである[21]。

Thus, the term "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour. By contrast, any personal data which have been created by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability.
したがって、「により提供された」という文言には、データ主体の活動に関する個人データ又は個人の行為の観察による個人データは含まれるが、その後の当該行動の分析結果のデータは含まれない。その一方で、データ管理者が、例えば個人化やレコメンデーション、ユーザーの分類別又はプロファイリングの過程などのデータ取扱いの一環として作成した個人データは、データ主体により提供された個人データから派生した又は推定されたデータであり、データポータビリティの権利の範囲に含まれない。

Third condition: the right to data portability shall not adversely affect the rights and freedoms of others.
第三の条件：データポータビリティの権利は他人の権利及び自由に不利な影響を与えてはならない。

With respect to personal data concerning other data subjects:
他のデータ主体に関する個人データについて:

The third condition is intended to avoid the retrieval and transmission of data containing the personal data of other (non-consenting) data subjects to a new data controller in cases where these data are likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects (Article 20(4) of the GDPR)[22].
第三の条件は、他の（同意のない）データ主体の個人データを含むデータが他のデータ主体

[21] This includes all data observed about the data subject during the activities for the purpose of which the data are collected, such as a transaction history or access log. Data collected through the tracking and recording of the data subject (such as an app recording heartbeat or technology used to track browsing behaviour) should also be considered as "provided by" him or her even if the data are not actively or consciously transmitted.
この範囲には、データ主体に関して、その個人データを収集した目的についての活動において観察される、取引履歴やアクセスログなどの全てのデータが含まれる。データ主体を（心拍記録アプリケーションや閲覧行為を追跡する技術などで）追跡し記録することで収集されたデータについても、その個人データが主体的に又は意思をもって移行されていなくても、「データ主体により提供された」データと見なされる。

の権利及び自由に不利な影響を与えるような方法で取扱われる可能性がある場合、こうしたデータの回収及び新たなデータ管理者への移行を避けることを意図している（GDPR 第20条(4)）[22]。

Such an adverse effect would occur, for instance, if the transmission of data from one data controller to another, would prevent third parties from exercising their rights as data subjects under the GDPR (such as the rights to information, access, etc.).
例えば、あるデータ管理者から別のデータ管理者へのデータの移行において、GDPRに基づくデータ主体としての第三者の権利行使（情報についての権利、アクセスなど）が妨げられれば、第三者の権利に対する不利な影響が生じうる。

The data subject initiating the transmission of his or her data to another data controller, either gives consent to the new data controller for processing or enters into a contract with that controller. Where personal data of third parties are included in the data set another legal basis for the processing must be identified. For example, a legitimate interest may be pursued by the data controller under Article 6(1)(f), in particular when the purpose of the data controller is to provide a service to the data subject that allows the latter to process personal data for a purely personal or household activity. The processing operations initiated by the data subject in the context of personal activity that concern and potentially impact third parties remain under his or her responsibility, to the extent that such processing is not, in any manner, decided by the data controller.
データ主体が自己の個人データを別のデータ管理者に移行する場合、データ主体は、その新たなデータ管理者がデータ取扱いを行うことに同意するか、当該管理者と契約を締結する。第三者の個人データが一連のデータに含まれる場合、取扱いに関し他の法的根拠が確認されなければならない。例えば、正当な利益は、第6条(1)(f)の規定に基づき、管理者によって追求されるが、特に、データ管理者の目的が、純粋に個人の又は家庭での活動のためにデータ主体による個人データの取扱いが認められているサービスをデータ主体に提供することにある場合が挙げられる。データ主体が個人的な活動の文脈で開始する、第三者に関連し、また、潜在的に影響を与える取扱いの実行については、当該取扱いがデータ管理者によって決定されない限り、いかなる方法であろうとも、当該データ主体の責任である。

[22] Recital 68 provides that "where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation."
前文第68項では、「個人データの一定のセットにおいて、二人以上のデータ主体が関係する場合、個人データを受領する権利は、その他のデータの主体の本規則に基づく権利の権利及び自由を侵害してはならない。」
と規定している。

For example, a webmail service may allow the creation of a directory of a data subject's contacts, friends, relatives, family and broader environment. Since these data relate to (and are created by) the identifiable individual that wishes to exercise his right to data portability, data controllers should transmit the entire directory of incoming and outgoing e-mails to that data subject.
例えば、ウェブメールサービスでは、データ主体の連絡先、友人、親類、家族や、より広い生活環境に関するディレクトリの作成が可能にしうる。こうしたデータは、データポータビリティの権利行使を望む特定可能な個人に関連している（また当該個人により作成された）データであるため、データ管理者は発信及び着信メールに関するディレクトリ全体を当該データ主体に移行するべきである。

Similarly, a data subject's bank account can contain personal data relating to the transactions not just of the account holder but also those of other individuals (e.g., if they have transferred money to the account holder). The rights and freedoms of those third parties are unlikely to be adversely affected by the transmission of the bank account information to the account holder once a portability request is made—provided that in both examples the data are used for the same purpose (i.e., a contact address only used by the data subject or a history of the data subject's bank account.
同様に、データ主体の銀行口座には、取引について、口座名義人個人データのみならず、他の個人の個人データも含みうる（例えば、第三者が口座名義人に送金した場合）。ポータビリティ要求が行われて口座名義人に銀行口座情報が移行されたとしても、いずれの例によってもデータが同じ目的に使われている場合（すなわち、連絡先やデータ主体の履歴がデータ主体によってのみ使用される場合）、この第三者の権利及び自由には、不利な影響が与えられる可能性が低い。

Conversely, the rights and freedoms of third parties will not be respected if the new data controller uses the personal data for other purposes, e.g. if the receiving data controller uses personal data of other individuals within the data subject's contact directory for marketing purposes.
逆に、新たなデータ管理者が、例えばデータ主体の連絡先ディレクトリにある他の個人のデータをマーケティングの目的に使うなど、その第三者の個人データを他の目的に使用する場合、第三者の権利及び自由は尊重されていないこととなる。

Therefore, to prevent adverse effects on the third parties involved, the processing of such personal data by another controller is allowed only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs. A receiving 'new' data controller (to whom the data can be transmitted at the request of the user) may not use the transmitted third party data for his own purposes e.g. to propose marketing products and services to those other third party data subjects. For example, this information should not be used to enrich the profile of

the third party data subject and rebuild his social environment, without his knowledge and consent[23]. Neither can it be used to retrieve information about such third parties and create specific profiles, even if their personal data are already held by the data controller. Otherwise, such processing is likely to be unlawful and unfair, especially if the third parties concerned are not informed and cannot exercise their rights as data subjects.

したがって、関連する第三者の権利に不利な影響を与えないために、別のデータ管理者によるそのような個人情報の取扱いが認められるのは、個人データを要求したユーザーのみによりデータが保存されている場合及び純粋に個人的に又は家庭での使用のためにデータが保存されている場合のみに限られる。データを受領する（ユーザーからの要求によりデータが移行される）「新たな」データ管理者は、移行されてきた第三者のデータを、他の第三者データ主体に対し市販製品やサービスを提案するなど、自己の目的のために使用できない。例えば、この情報は、第三者データ主体が知ることなく、かつ、同意なく、当該第三者データ主体のプロファイルを改良し、またその社会的環境を再構築するために使用されるべきではない[23]。この情報は、また、データ管理者が当該第三者データ主体の個人データを既に保有しているとしても、当該第三者データ主体に関する情報を抽出し、特定のプロファイルを作成するためにも使用してはならない。かかる使用をした場合、関連のある第三者が取扱いについて知らされておらずデータ主体としてその権利を行使できない場合は特に、当該取扱いは違法又は不正である可能性がある。

Furthermore, it is a leading practice for all data controllers (both the "sending" and "receiving" parties) to implement tools to enable data subjects to select the relevant data they wish to receive and transmit and exclude, where relevant, data of other individuals. This will further assist in reducing the risks for third parties whose personal data may be ported.

さらに、（「移行元」側及び「移行先」側双方の）全てのデータ管理者にとって、データ主体が受領及び移行を望む関連データを選択し、関連する場合には他の個人のデータを除外できる手段を実施することは指導的な慣行である。 これは、移行されうる個人データのデータ主体となる第三者にとってのリスクの減少をより助けるものである。

Additionally, the data controllers should implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent, e.g. if they also want to move their data to some other data controller. Such a situation might arise, for example, with social networks, but it is up to data controllers to decide on the leading practice to follow.

[23] A social networking service should not enrich the profile of its members by using personal data transmitted by a data subject as part of his right to data portability, without respecting the principle of transparency and also making sure they rely on an appropriate legal basis regarding this specific processing.
ソーシャルネットワークサービスは、透明性の原則を尊重することなしに、また、特定の取扱いについての適切な法的根拠に基づくことを確保せずに、あるデータ主体からのデータポータビリティの権利の行使によって移行された個人データを用いて自己の会員のプロファイルを改良するべきではない。

これに加え、データ管理者は、例えば、関連のある他のデータ主体もまた、自己のデータを別のデータ管理者への移行を望む場合など、当該関連のある他のデータ主体が自ら同意することを望む場合にデータ移行を容易にするため、こうした他のデータ主体から同意を得るための仕組みを実施すべきである。こうした状況は、例えば、ソーシャルネットワークで生じうるが、指導的な慣行に従うかを決定するのはデータ管理者次第である。

With respect to data covered by intellectual property and trade secrets:
知的財産及び営業秘密に該当するデータについて:

The rights and freedoms of others are mentioned in Article 20(4). While not directly related to portability, this can be understood as "including trade secrets or intellectual property and in particular the copyright protecting the software. However, even though these rights should be considered before answering a data portability request, "the result of those considerations should not be a refusal to provide all information to the data subject". Furthermore, the data controller should not reject a data portability request on the basis of the infringement of another contractual right (for example, an outstanding debt, or a trade conflict with the data subject).
他人の権利及び自由は第 20 条(4)で言及されている。これはポータビリティには直接関連しないが、「営業秘密又は知的財産及び特にソフトウェアを保護している著作権を含む」［訳注：GDPR 前文第 63 項にある文言に該当］と解しうる。しかしながら、データポータビリティの要求への対応に先立ってこうした権利が考慮されるべきであるとしても、「こうした考慮の結果が、データ主体に対する全ての情報の提供拒否となるべきではない」。さらに、データ管理者は、他の契約上の権利の侵害（例：データ主体との未払債務又は取引にかかる紛争）を根拠として、データポータビリティの要請を拒否すべきではない。

The right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights. **A potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request** and data controllers can transmit the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.
データポータビリティの権利は、個人が、不正行為と見なされうる方法で、又は知的財産権を侵害する方法で、情報を悪用するための権利ではない。**しかしながら、事業にリスクが伴うということだけでは、データポータビリティの要求を拒否する根拠にはならない。**データ管理者は、データ主体により提供された個人データを、営業秘密又は知的財産権に該当する情報を除く形式で移行することができる。

IV. How do the general rules governing the exercise of data subject rights apply to data portability?

IV. データ主体の権利行使の一般原則はどのようにデータポータビリティに適用されるか？

- **What prior information should be provided to the data subject?**
- **データ主体には事前にどのような情報が提供されるべきか？**

In order to comply with the new right to data portability, data controllers must inform data subjects of the existence of the new right to portability. Where the personal data concerned are directly collected from the data subject, this must happen "at the time where personal data are obtained". If the personal data have not been obtained from the data subject, the data controller must provide the information as required by Articles 13(2)(b) and 14(2)(c).

新たなデータポータビリティの権利を遵守するために、データ管理者は、データ主体に対し、新たなデータポータビリティの権利の存在を通知しなければならない。関連する個人データがデータ主体から直接収集される場合には、このことは「個人データが取得されるとき」になされなければならない。個人データがデータ主体から取得されなかった場合には、データ管理者は、第 13 条(2)(b)及び第 14 条(2)(c)の定めに従い、情報を提供しなければならない。

"Where the personal data have not been obtained from the data subject", Article 14(3) requires the information to be provided within a reasonable time not exceeding one month after obtaining the data, during first communication with the data subject, or when disclosure is made to third parties[24].

「個人データがデータ主体から取得されていない場合」、第 14 条(3)は、当該データの取得後 1 か月を超えない合理的な期間内、データ主体との当初の連絡した時点、又は第三者に開示するとき、に情報を提供するよう要求している[24]。

When providing the required information data controllers must ensure that they distinguish the right to data portability from other rights. Therefore, WP29 recommends in particular that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability.

要求された情報を提供する際、データ管理者は、データポータビリティの権利と他の権利を確実に区別できるようにしなければならない。したがって、WP29 は、特に、データ主体が

[24] Article 12 requires that data controllers provide "any communications […] in a concise, transparent, intelligible, and easily assessable form, using clear and plain language, in particular for any information addressed specifically to a child."
第 12 条は、データ管理者が「いかなる通知について[...]特に子供に対しての情報について、明瞭かつ平易な文言が使われ、簡潔で、透明性があり、理解し易く、かつ容易にアクセスしうる形式で」提供することを求めている。

そのアクセス権及びデータポータビリティの権利を通じて取得できるデータの種類の差異についてデータ管理者が明確に説明するよう提言する。

In addition, the Working Party recommends that data controllers always include information about the right to data portability before data subjects close any account they may have. This allows users to take stock of their personal data, and to easily transmit the data to their own device or to another provider before a contract is terminated.
さらに、WP29 は、データ管理者に対し、データ主体が保有しているであろうアカウントをデータ主体が閉鎖するに先立ち、常にデータポータビリティの権利に関する情報を含めるよう提言する。これにより、ユーザーは、契約終了前に、自己の個人データを確認し、自己の装置に又は別の役務提供事業者にそのデータを容易に移行することができる。

Finally, as leading practice for "receiving" data controllers, the WP29 recommends that data subjects are provided with complete information about the nature of personal data which are relevant for the performance of their services. In addition to underpinning fair processing, this allows users to limit the risks for third parties, and also any other unnecessary duplication of personal data even where no other data subjects are involved.
最後に、データを「受領する」データ管理者の指導的な慣行として、WP29 は、サービスの実施に関連する個人データの性質について、完全な情報がデータ主体に提供されるよう提言する。これにより、公正な取扱いが支えられることに加え、ユーザーは、第三者に対するリスクを限定し、また、たとえ他のデータ主体が関わっていないとしても、個人データの不要な複製を限定することができる。

- **How can the data controller identify the data subject before answering his request?**
- **要求に対応する前にデータ管理者はどのようにデータ主体を特定できるか？**

There are no prescriptive requirements to be found in the GDPR on how to authenticate the data subject. Nevertheless, Article 12(2) of the GDPR states that the data controller shall not refuse to act on request of a data subject for exercising his or her rights (including the right to data portability) unless it is processing personal data for a purpose that does not require the identification of a data subject and it can demonstrate that it is not able to identify the data subject. However, as per Article 11(2), in such circumstances the data subject can provide more information to enable his or her identification. Additionally, Article 12(6) provides that where a data controller has reasonable doubts about the identity of a data subject, it can request further information to confirm the data subject's identity. Where a data subject provides additional information enabling his or her identification, the data controller shall not refuse to act on the request. Where information and data collected online is linked

to pseudonyms or unique identifiers, data controllers can implement appropriate procedures enabling an individual to make a data portability request and receive the data relating to him or her. In any case, data controllers must implement an authentication procedure in order to strongly ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR.

GDPR には、データ主体の本人認証に関する規範的要件はない。とはいえ、GDPR 第 12 条(2)では、データ管理者がデータ主体の特定を不要とする目的のために個人データを取扱っており、またデータ管理者がそのデータ主体を特定できないことを証明した場合を除き、データ管理者は、（データポータビリティの権利を含む）権利の行使についてデータ主体から要求があった場合、その対応を拒否してはならないと規定している。しかしながら、第 11 条(2)に規定されているように、そのような場合は、データ主体は自己の特定を可能とするためにより多くの情報を提供することができる。これに加え、第 12 条(6)では、データ管理者がデータ主体の身元について合理的な疑いを有する場合、データ管理者はそのデータ主体の身元を確認するためにより多くの情報の提供を要求できることが規定されている。データ主体が自己の特定を可能とする追加の情報を提供する場合、データ管理者はデータポータビリティの要求への対応を拒否してはならない。インターネット上で収集された情報及びデータが仮名の又は独自の識別子に関連付けられている場合、データ管理者は適切な手順を実行し、個人がデータポータビリティの要求を行い自己に関する個人データを取得できるようにすることができる。いずれにせよ、データ管理者は個人データを要求するデータ主体、又はより一般的に、GDPR において付与されている権利を行使するデータ主体の本人性を確実に確認するために、本人認証手続を実施しなければならない。

These procedures often already exist. The data subjects are often already authenticated by the data controller before entering into a contract or collecting his or her consent to the processing. As a consequence, the personal data used to register the individual concerned by the processing can also be used as evidence to authenticate the data subject for portability purposes[25].

これらの手続は、しばしば、既に存在しているものである。データ主体は、しばしば、データ管理者から、契約の締結前、又は取扱いに対する同意を得る前に、既に本人認証を受けている。結果として、当該取扱いによって、当該個人の登録に使用された個人データは、ポータビリティの目的上、データ主体を認証する証拠としても使用されうる[25]。

While in these cases, the data subjects' prior identification may require a request for proof of their legal identity, such verification may not be relevant to assess the link between the data and the

[25] For example, when the data processing is linked to a user account, providing the relevant login and password might be sufficient to identify the data subject.
例えば、データ取扱いがユーザーアカウントと結びついている場合には、関連するログインとパスワードを提供することがデータ主体の認証に十分でありうる。

individual concerned, since such a link is not related with the official or legal identity. In essence, the ability for the data controller to request additional information to assess one's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.
これらの事例においては、データ主体の事前認証に法的な身分の証明の要求が必要となろうが、そのような証明は、当該データと当該個人間のつながりを評価することとは、当該つながりが公的な又は法的な本人性と関連しないため、関係ないであろう。要するに、データ管理者が個人の本人性を評価するための追加情報を求めることができることは、過度の要求や、個人と要求された個人データ間のつながりの強化に関連しない又は必要のない個人データの収集と結び付けることはできない。

In many cases, such authentication procedures are already in place. For example, usernames and passwords are often used to allow individuals to access their data in their email accounts, social networking accounts, and accounts used for various other services, some of which individuals chose to use without revealing their full name and identity.
多くの場合、このような認証手続はかねてから実施されている。例えば、ユーザー名とパスワードは、しばしば各個人が、電子メールアカウント、ソーシャルネットワークのアカウント及び他の様々なサービスに用いられているアカウントにおける自己のデータを入手できるようにするために使われる。こうした個人の中には、自己の名前や身元を明かさないでこれを使用する者もいる。

If the size of data requested by the data subject makes transmission via the internet problematic, rather than potentially allowing for an extended time period of a maximum of three months to comply with the request[26], the data controller may also need to consider alternative means of providing the data such as using streaming or saving to a CD, DVD or other physical media or allowing for the personal data to be transmitted directly to another data controller (as per Article 20(2) of the GDPR where technically feasible).
データ主体により要求されたデータサイズが、要求を遵守するための最長 3 か月までの延長期間[26]を要するというよりも、インターネット経由での移行に問題を生じさせることになる場合、データ管理者は、そのデータの提供方法について、ストリーミングの利用、CD、DVD などの物理的媒体の使用、又はデータ主体から許可をもらい個人データを別のデータ管理者に直接移行する、などの代替手段を考慮する必要もありうる（GDPR 第 20 条(2)に従い、技術的に実行可能な場合）。

[26] Article 12(3): "The controller shall provide information on action taken on a request".
第 12 条(3)：「データ管理者は要求に対してとられた行為に関する情報を提供するべきである」

- **What is the time limit imposed to answer a portability request?**
- **データポータビリティの要求への対応期限はいつか？**

Article 12(3) requires that the data controller provides "information on action taken" to the data subject "without undue delay" and in any event "within one month of receipt of the request". This one month period can be extended to a maximum of three months for complex cases, provided that the data subject has been informed about the reasons for such delay within one month of the original request.
第 12 条(3)では、データ管理者は、データ主体に対し「とられた行為に関する情報」を「不当に遅延することなく」、そして、いずれにしても、「要求の受領より 1 か月以内に」提供することが義務付けられている。この 1 か月という期間は、複雑なケースで、データ主体が最初の要求から 1 か月以内に遅延理由を通知されていれば、最長で 3 か月まで延長できる。

Data controllers operating information society services are likely to be better equipped to be able to comply with requests within a very short time- period. To meet user expectations, it is a good practice to define the timeframe in which a data portability request can typically be answered and communicate this to data subjects.
情報社会サービスを運営しているデータ管理者は、非常に短期間で要求に応じることができる設備が整っている可能性が高い。ユーザーの期待に応えるために、データポータビリティの要求について通常の対応にかかる期間を明確にし、これをデータ主体に伝えることは望ましい慣行である。

Data controllers who refuse to answer a portability request shall , pursuant to Article 12(4), inform the data subject "the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy", no later than one month after receiving the request.
データポータビリティの要求への対応を拒むデータ管理者は、第 12 条(4)に従い、データ主体に対し、「対応を拒む理由、及び監督機関に不服申立てを行い法的救済を求めることができる」旨を、要求の受領後 1 か月以内に通知しなければならない。

Data controllers must respect the obligation to respond within the given terms, even if it concerns a refusal. In other words, the data controller cannot remain silent when it is asked to answer a data portability request.
データ管理者は、たとえ要求を拒むことを考えているとしても、規定の期間内に対応する義務を遵守する必要がある。つまり、データ管理者は、データポータビリティの要求に対応するよう求められた場合、沈黙したままであってはならない。

- **In which cases can a data portability request be rejected or a fee charged?**
- **どのような場合にデータポータビリティの要求を拒否し、又は手数料を課してもよいか？**

Article 12 prohibits the data controller from charging a fee for the provision of the personal data, unless the data controller can demonstrate that the requests are manifestly unfounded or excessive, "*in particular because of their repetitive character*". For information society services that specialise in automated processing of personal data, implementing automated systems such as Application Programming Interfaces (APIs)[27] can facilitate the exchanges with the data subject, hence lessen the potential burden resulting from repetitive requests. Therefore, there should be very few cases where the data controller would be able to justify a refusal to deliver the requested information, even regarding multiple data portability requests.

第 12 条では、データ管理者がそのデータポータビリティの要求に明らかに根拠がないこと、又は過度であり、「特に反復的な性質であるため」であることを証明できる場合を除き、データ管理者が個人データの提供に手数料を課すことは禁じられている。個人データの自動取扱いを専門としている情報社会サービスについては、アプリケーション・プログラミング・インターフェイス（APIs）[27]のような自動化されたシステムの実施は、データ主体との交換を促進させることができ、それゆえ、繰り返される要求から生じる負担を軽減させる。したがって、データ管理者が、データポータビリティの要求が複数あるとしても、要求された情報の提供を正当に拒否できるケースは極めて少ない。

In addition, the overall cost of the processes created to answer data portability requests should not be taken into account to determine the excessiveness of a request. In fact, Article 12 of the GDPR focuses on the requests made by one data subject and not on the total number of requests received by a data controller. As a result, the overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests.

さらに、データポータビリティの要求への対応について作られるプロセス全体の費用は、ある要求が過度であるか否かを決定する場合に考慮すべきでない。実際に、GDPR 第 12 条は、データ管理者が受領した要求の総数でなく、一のデータ主体が行った複数の要求に焦点を当てている。結果として、システム全体での実施費用は、データ主体に課してはならず、また、データポータビリティの要求への対応の拒否を正当化する理由にもならない。

[27] Application Programming Interface (API) means the interfaces of applications or web services made available by data controllers so that other systems or applications can link and work with their systems.
アプリケーション・プログラミング・インターフェース（API）は、データ管理者が自らのシステムと他のシステムやアプリケーションを接続し又は連携できるアプリケーションのインターフェース若しくはウェブサービスを意味する。

V. How must the portable data be provided?
V. ポータブルデータはどのように提供されるべきか？

- **What are the expected means the data controller should implement for data provision?**
- データ管理者に求められるデータの提供方法は何か？

Article 20(1) of the GDPR provides that data subjects have the right to transmit the data to another controller without hindrance from the controller to which the personal data have been provided.
GDPR 第 20 条(1)では、データ主体は、データを提供した管理者の妨害なく、データを他の管理者に移行する権利を有すると規定している。

Such hindrance can be characterised as any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller. For example, such hindrance could be: fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate obfuscation of the dataset, or specific and undue or excessive sectorial standardization or accreditation demands[28].
このような妨害は、データ管理者がデータ主体や他のデータ管理者によるアクセス、移行又は再利用を止めさせる又は遅延させるために行うあらゆる法的、技術的又は金銭的妨害と特徴づけることができる。例えば、そのような妨害には、データ提供に要求される手数料、データ形式、API 又は提供された形式についての相互運用可能性又はアクセスの欠如、全データセットの取り出しにおける過度の遅延又は複雑さ、データセットの意図的な難読化、又は、特定かつ不当な又は過度の部門別標準化又は認定の要求があろう[28]。

Article 20(2) also places obligations on data controllers for transmitting the portable data directly to other data controllers “when technically feasible”.
第 20 条(2)は、データ管理者に対し、「技術的に実現可能な場合」に、ポータブルデータを直接他のデータ管理者に移行することにつき義務も課している。

[28] Some legitimate obstacles might arise, as the ones, which are related to the rights and freedoms of others mentioned in Article 20(4), or the ones that relate to the security of the controllers’ own systems. It shall be the responsibility of the data controller to justify why such obstacles would be legitimate and why they do not constitute a hindrance in the meaning of Article 20(1).
第 20 条(4)に規定された第三者の権利及び自由に関連するもの、又は管理者の自己のシステムの安全性に関連するものなど、何らかの正当な障害は生じるかもしれない。なぜこのような障害が正当なものであって第 20 条(1)の妨害に該当しないのかについては、データ管理者が正当性を立証する責任を有するべきである。

The technical feasibility of transmission from data controller to data controller, under the control of the data subject, should be assessed on a case by case basis. Recital 68 further clarifies the limits of what is "technically feasible", indicating that "it should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible".
データ主体のコントロール下におけるデータ管理者からデータ管理者への移行における技術的な実現可能性は、ケース・バイ・ケースで判断されるべきである。前文第 68 項では、「技術的に実現可能」の限界をさらに明確にしており、「データ管理者に対し技術的に互換性のある取扱いシステムの導入又は維持の義務を負わせるものではない」と述べている。

Data controllers are expected to transmit personal data in an interoperable format, although this does not place obligations on other data controllers to support these formats. Direct transmission from one data controller to another could therefore occur when communication between two systems is possible, in a secured way[29], and when the receiving system is technically in a position to receive the incoming data. If technical impediments prohibit direct transmission, the data controller shall explain those impediments to the data subjects, as his decision will otherwise be similar in its effect to a refusal to take action on a data subject's request (Article 12(4)).
データ管理者は、個人データを相互運用可能な形式で移行することを期待されている。もっとも、このことは、他のデータ管理者に対しそのような形式をサポートする義務を課すものではない。したがって、あるデータ管理者から他のデータ管理者への直接の移行は、二つのシステム間の通信が安全な方法[29]で可能であり、受領側のシステムが技術的に移行データを受領できる状況にある場合に、生じうる。技術的障害により直接の移行ができない場合には、データ管理者は、その旨説明をしなかった場合には自己の決定の効果がデータ主体の要求に対し措置を採ることを拒否したのと同様になるため、データ主体に対しその障害を説明しなければならない（第 12 条(4)）。

On a technical level, data controllers should explore and assess two different and complimentary paths for making portable data available to the data subjects or to other data controllers:

- a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset);

[29] Through an authenticated communication with the necessary level of data encryption.
必要なレベルのデータ暗号化がされている認証された通信を通じて。

- an automated tool that allows extraction of relevant data.

データ管理者は、技術的なレベルにおいて、データ主体又は他のデータ管理者がポータブルデータを利用できるようにするよう、二つの異なる補完的な手法を検討し評価すべきである。

- ポータブルデータの全体のデータセットの直接移行（又はグローバル・データセットの部分からの複数の抽出）
- 関連データの抽出を可能にする自動化されたツール

The second way may be preferred by data controllers in cases involving of complex and large data sets, as it allows for the extraction of any part of the data-set that is relevant for the data subject in the context of his or her request, may help minimising risk, and possibly allows for use of data synchronisation mechanisms[30] (e.g. in the context of a regular communication between data controllers). It may be a better way to ensure compliance for the "new" data controller, and would constitute good practice in the reduction of privacy risks on the part of the initial data controller.
二つ目の方法は、データ主体の要求に関連するデータセットのいかなる部分をも抽出可能とし、リスクを軽減させる可能性があり、また、データ同期化メカニズムの使用（例えば、データ管理者間における定期的な連絡の文脈において）を可能としうることから、複雑かつ大量のデータセットが含まれる場合にデータ管理者が好むであろう[30]。この方法は「新」データ管理者のコンプライアンスを確保するためのより良い方法であろうし、元々のデータ管理者のプライバシーリスクの軽減における望ましい慣行となろう。

These two different and possibly complementary ways of providing relevant portable data could be implemented by making data available through various means such as, for example, secured messaging, an SFTP server, a secured WebAPI or WebPortal. Data subjects should be enabled to make use of a personal data store, personal information management system[31] or other kinds of trusted third-parties, to hold and store the personal data and grant permission to data controllers to access and process the personal data as required.
これら二つの異なった、そして、おそらく補完的な、関連するポータブルデータの提供方法

[30] Synchronisation mechanism can help reaching the general obligations under Article 5obligation of the GDPR, which provides that "personal data shall be (…) accurate and, where necessary, kept up to date"
データ同期化メカニズムは、GDPR 第 5 条の「パーソナルデータは(…)正確であり、かつ必要である場合には最新であるべきである」という一般的義務を達成する手助けとなりうる。
[31] On personal information management systems (PIMS), see, for example, EDPS Opinion 9/2016, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf
個人情報管理システム（PIMS）について、例えば以下の EDPS Opinion 9/2016 を参照。
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

は、例えば、安全が保証されたメッセージング、SFTP サーバー、安全が保証されたウェブ API 又はウェブポータルなど、様々な手段を通じてデータを利用可能とさせることにより実行できるであろう。データ主体は、個人データを保有・保存し、要求に応じて、データ管理者に対し当該個人データへのアクセス及び取扱いの許可を与えるため、個人データストア、個人情報管理システム [31] 又は他の種類の委託された第三者の利用ができるようにすべきである。

- **What is the expected data format?**
- **期待されるデータ形式は何か？**

The GDPR places requirements on data controllers to **provide the personal data requested by the individual in a format, which supports re-use**. Specifically, Article 20(1) of the GDPR states that the personal data must be provided "in a structured, commonly used and machine readable format". Recital 68 provides a further clarification that this format should be interoperable, a term that is defined[32] in the EU as:

GDPR では、データ管理者は、**個人から要求された個人データを、再利用をサポートする形式で提供する**ことが義務付けられている。具体的には、GDPR 第 20 条(1)では、個人データは「構造化され、一般的に使用され、機械可読性のある形式で」提供されなければならないと規定している。前文第 68 項では、これをさらに明確にし、この形式は、「相互運用可能」な形式でなければならないと規定しているこの「相互運用可能」については EU において以下のように定義されている[32]。

> *the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.*
> *異種及び多様な組織が、組織間の情報及び知識の共有を含む互恵的かつ同意された共通の目標を目指し、各組織が支援する事業プロセスを通じ、各 ICT システム間でのデータ交換手段を用いて、相互に交流できること。*

The terms "structured", "commonly used" and "machine-readable" are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller. In that way,

[32] Article 2 of Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) OJ L 260, 03.10.2009, p. 20
2009 年 9 月 16 日、欧州行政組織のための相互運用性ソリューション（ISA)に関する、欧州議会及び理事会決定第 922/2009/EC 第 2 条（OJ L260、03.10.2009、p.20）

"structured, commonly used and machine readable" are specifications for the means, whereas interoperability is the desired outcome.
「構造化された」、「一般的に利用される」、「機械可読性のある」という文言は、データ管理者により提供されるデータ形式の相互運用性を促進する、最低限の要件である。この点において、「構造化され、一般的に利用され機械可読性のある」という文言は、手段の仕様であり、相互運用性は望ましい結果である。

Recital 21 of Directive 2013/37/EU[3334] defines "machine readable" as:
2013/37/EU17 指令前文第 21 項 [3334] では、「機械可読性のある」("machine readable") について次のように定義している。

> *a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats.*
> *ソフトウェアアプリケーションが個人の事実記載を含む特定のデータ及びその内部構造を容易に特定、認識及び抽出できるよう構造化されているファイルフォーマットである。機械可読性のある形式で構造化されているファイルの符号化されたデータは、機械可読性のあるデータである。機械可読性のある形式は、公開又は独占的な形式であり得、公式な標準形式である場合とそうでない場合がある。自動取扱いを制限するファイル形式で符号化されている文書については、文書からのデータ抽出が不可能又は容易でないため、機械可読な形式でないとみなされる。加盟国は、適切な場合、公開されている、機械可読な形式の利用を促進すべきである。*

Given the wide range of potential data types that could be processed by a data controller, the GDPR does not impose specific recommendations on the format of the personal data to be provided. The most appropriate format will differ across sectors and adequate formats may already exist, and should always be chosen to achieve the purpose of being interpretable and affording the data subject with a

[33] Amending Directive 2003/98/EC on the re-use of public sector information.
公的部門の情報の再利用に関する指令（2003/98/EC）に係る改正
[34] The EU glossary (http://eur-lex.europa.eu/eli-register/glossary.html) provides further clarification on expectations related to the concepts used in this guideline, such as *machine-readable*, *interoperability*, *open format*, *standard*, *metadata*.
EU 用語集 (http://eur-lex.europa.eu/eli-register/glossary.html)は、*機械可読性*（*machine-readable*）、*相互運用性*（*interoperability*）、*オープンフォーマット*（*openformat*）、*基準*（*standard*）、*メタデータ*（*metadata*）など本ガイドラインで使われている概念に関連した期待について更なる明確化を提供している。

large degree of data portability. As such, formats that are subject to costly licensing constraints would not be considered an adequate approach.
GDPR では、データ管理者により取扱われる可能性のあるデータの種類が広範囲に渡ることを考慮し、提供される個人データの形式については特に提言されていない。最適な形式は産業分野によって異なり、適切な形式は既に存在しているかもしれず、また、解釈が可能でデータ主体に大きなポータビリティを与える目的を達成するための形式が常に選択されるべきである。コストのかかるライセンス契約の制約がある形式は、適切な方法とみなされない。

Recital 68 clarifies that "*The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.*" **Thus, portability aims to produce interoperable systems, not compatible systems[35].**
前文第 68 項では、「データ主体に関する個人データを本人が移行又は受領する権利は、管理者に技術的に互換性のある取扱システムを採用又は保守する義務を負わせるものではない」ことが明示されている。**したがって、データポータビリティは、互換性のあるシステムでなく、相互運用可能なシステムを生み出すことを意図している[35]。**

Personal data are expected to be provided in formats that have a high level of abstraction from any internal or proprietary format. As such, data portability implies an additional layer of data processing by data controllers, in order to extract data from the platform and filter out personal data outside the scope of portability, such as inferred data or data related to security of systems. In this way, data controllers are encouraged to identify beforehand data which are within the scope of portability in their own systems. This additional data processing will be considered as ancillary to the main data processing, since it is not performed to achieve a new purpose defined by the data controller.
個人データは、いかなる内部仕様又は独自仕様の形式よりも高度に抽象化された形式で提供されることが期待される。このように、データポータビリティは、プラットフォームからデータを抽出し、データポータビリティの範囲に該当しない推測データ又はシステムの安全に関連するデータなどの個人データを除外するための、データ管理者による追加的な取扱いを示唆している。この方法により、データ管理者は、自己のシステムにおいてポータビリティの範囲内のデータを、あらかじめ特定するよう促される。この追加的なデータ取扱いは、データ管理者により定められた新たな目的を達成するために遂行されるものではないため、主なデータ取扱いの補助的な取扱いと見なされる。

[35] ISO/IEC 2382-01 defines interoperability as follows: "The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units."
ISO/IEC 2382-01 において、相互運用性は次のように定義されている。
「様々な機能装置間で通信し、プログラムを履行し、データを伝達できることであって、これは、ユーザーが、こうした装置の独自の特徴に関する知識を有する必要が全くない状況において実施される。」

Where no formats are in common use for a given industry or given context, data **controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,…) along with** useful **metadata at the best possible level of granularity,** while maintaining a high level of abstraction. As such, suitable metadata should be used in order to accurately describe the meaning of exchanged information. This metadata should be enough to make the function and reuse of the data possible but, of course, without revealing trade secrets. It is unlikely therefore that providing an individual with PDF versions of an email inbox would be sufficiently structured or descriptive to allow the inbox data to be easily reused. Instead, the e-mail data should be provided in a format which preserves all the metadata, to allow the effective re-use of the data. As such, when selecting a data format in which to provide the personal data, the data controller should consider how this format would impact or hinder the individual's right to re-use the data. In cases where a data controller is able to provide choices to the data subject regarding the preferred format of the personal data a clear explanation of the impact of the choice should be provided. However, processing additional metadata for the sole purpose that they might be needed or wanted to answer a data portability request poses no legitimate ground for such processing.

ある産業又はある状況において通常使用されている形式がない場合、データ管理者は、個人データを、一般に使用されているオープンフォーマット（例えば、XML、JSON、CSV など）を有用な**メタデータと共に使用して、できる限り最良の粒度で、**ただ高度の抽象化を維持しつつ、**提供すべきである。**だからこそ、交換される情報の意味を正確に記述するために、適切なメタデータが使用されるべきである。このメタデータは、当該データが機能すること及びその再利用を可能とするに十分なもの（もっとも、もちろん営業秘密を公開することなく）であるべきである。したがって、個人に電子メールの受信データを PDF 形式で提供することは、その受信データを容易に再利用できるようにするのに十分に構造化され又は記述的であるとはいえないであろう。その代わり、 電子メールのデータは、データの効率的な再利用を可能にするよう全てのメタデータを保持する形式で提供されるべきである。このように、データ管理者は、個人データを提供するデータ形式を選ぶ際、その形式が、データを再利用する個人の権利についてどのように影響を与えるか、又は権利の障害となるかを考慮すべきである。データ管理者が、個人データの好ましい形式についてデータ主体が選択できるようにする場合、その選択が与える影響を明確に説明すべきである。しかしながら、データポータビリティの要求に応じるためにメタデータが必要とされる又は希望されるであろうという目的のみでメタデータをさらに取扱う場合、その取扱いには正当な理由がない。

WP29 strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the

requirements of the right to data portability. This challenge has also been addressed by the European Interoperability Framework (EIF) which has created an agreed approach to interoperability for organizations that wish to jointly deliver public services. Within its scope of applicability, the framework specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices[36].

WP29 は、産業界関係者と事業者団体とがデータポータビリティの権利の要件を遵守するために、協力して、統一した相互運用基準及び形式の策定に取り組むことを強く促す。この課題は、また、欧州相互運用化構想 （European Interoperability Framework：EIF）により協議されており、EIF では、共同した公的サービスの提供を望む機関のための相互運用性に関して合意されたアプローチを作成した。適用範囲について、この構想では、語彙、概念、原則、方針、ガイドライン、提言、基準、仕様及び慣行など、一連の共通する構成要素が具体化されている[36]。

- **How to deal with a large or complex personal data collection?**
- **大量又は複雑なデータ群をどのように取扱うか？**

The GDPR does not explain how to address the challenge of responding where a large data collection, a complex data structure or other technical issues arise that might create difficulties for data controllers or data subjects.

GDPR では、大量のデータ収集、複雑なデータ構造又はその他の技術問題により生じうるデータ管理者やデータ主体の困難についてどのように対処するかの解決策は説明されていない。

However, in all cases, it is crucial that the individual is in a position to fully understand the definition, schema and structure of the personal data that could be provided by the data controller. For instance, data could first be provided in a summarised form using dashboards allowing the data subject to port subsets of the personal data rather than the entirety. The data controller should provide an overview "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (see Article 12(1)) of the GDPR) in such a way that data subject should always have clear information of what data to download or transmit to another data controller in relation to a given purpose. For example, data subjects should be in a position to use software applications to easily identify, recognize and process specific data from it.

しかしながら、いかなる場合でも、各個人が、データ管理者により提供される個人データの定義、概要及び構造を完全に理解する立場にあることが重要である。例えば、データは最初、

[36] Source: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf
出典：http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

データ主体が個人データのサブセットを移植できるように、完全な形ではなく、ダッシュボードを利用した要約形式で提供されうる。データ管理者は、データ主体が所与の目的に関連して、どのデータをダウンロードし、又は他のデータ管理者に移行するかにつき常に明確な情報を持つよう、「明瞭かつ平易な文言が使われ、簡潔で、透明性があり、理解しやすくかつ容易にアクセスしうる形式で」（GDPR 第 12 条(1)を参照）要旨を提供すべきである。例えば、データ主体は、特定のデータを容易に特定、認識及び処理できるようソフトウェアアプリケーションを使用できる状況にあるべきである。

As referenced above, a practical way by which a data controller can answer requests for data portability may be by offering an appropriately secured and documented API. This may enable individuals to make requests of the data controller for their personal data via their own or third-party software or grant permission for others to so do on their behalf (including another data controller) as specified in Article 20(2) of the GDPR. By granting access to data via an externally accessible API, it may also be possible to offer a more sophisticated access system that enables individuals to make subsequent requests for data, either as a full download or as a delta function containing only changes since the last download, without these additional requests being onerous on the data controller.
上述のように、データ管理者がデータポータビリティの要求に対応できる実践的な方法は、適切に安全性が確保され、書面化された API を提供することかもしれない。 この方法により、個人は、データ管理者に対し、自己又は第三者のソフトウェアを通じて自己の個人データを要求又は GDPR 第 20 条(2)の規定に基づき、他人（別のデータ管理者を含む）に自己に代わって要求することについて許可を与えることができる。外部からアクセス可能な API 経由でのデータへのアクセスを許可することで、個人がその後も、データ管理者の負担となる追加要求を行うことなく、全体のダウンロードか変更箇所のみ記載されているデルタ関数の何れかの形でデータを要求できる、より高度なアクセスシステムの提供も可能となりうる。

- **How can portable data be secured?**
- **どのようにポータブルデータの安全性を確保できるか？**

In general, data controllers should guarantee the "appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures" according to Article 5(1)(f) of the GDPR.
一般的に、データ管理者は、GDPR 第 5 条(1)(f)の規定によれば、「個人データについて、適切な技術的又は組織的方策により、不正又は違法な取扱いからの保護及び偶発的な損失、破壊又は損害からの保護を含む、そのデータの適切な安全性」を保証するべきである。

However, the transmission of personal data to the data subject may also raise some security issues:
しかしながら、個人データのデータ主体への移行においては、安全性に問題が生じる場合がある。

How can data controllers ensure that personal data are securely delivered to the right person?
データ管理者は個人データの適切な者への安全な送信をどのように担保できるのか？

As data portability aims to get personal data out of the information system of the data controller, the transmission may become a possible source of risk regarding those data (in particular of data breaches during the transmission). The data controller is responsible for taking all the security measures needed to ensure not only that personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures), but also continuing to protect the personal data that remains in their systems, as well as transparent procedures for dealing with possible data breaches[37]. As such, data controllers should assess the specific risks linked with data portability and take appropriate risks mitigation measures.
データポータビリティは、データ管理者の情報システムから個人データを取り出すことを目的としているため、こうしたデータについては、移行が（特に、移行中のデータ漏えいについて）リスク源となる可能性がある。データ管理者は、個人データが正しい宛先（強力な認証手続により）に（全面的あるいはデータの暗号化により）安全に移行されるのみならず、自己のシステムに残存する個人データの継続的な保護を確実にするために必要とされるあらゆる安全対策を講じる責任を有し、また、起こりうるデータ漏えい[37]への対処に係る透明性のある手続をとる責任を有する。したがって、データ管理者は、データポータビリティに関連する特定のリスクを査定し、適切なリスク軽減策を採るべきである。

Such risk mitigation measures could include: if the data subject already needs to be authenticated, using additional authentication information, such as a shared secret, or another factor of authentication, such as a onetime password; suspending or freezing the transmission if there is suspicion that the account has been compromised; in cases of a direct transmission from a data controller to another data controller, authentication by mandate, such as token-based authentications, should be used.
このようなリスク軽減策には、次のものが含まれうる。データ主体が既に認証を必要とする

[37] In conformance to the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
EUにおける高い共通レベルのネットワークセキュリティ及び情報システムについての方法に関するDirective (EU) 2016/1148と適合する。

場合に、例えば、共有秘密や、ワンタイムパスワードなど認証における別の要素を使用すること。アカウント漏えいの疑いがある場合に移行を中止又は凍結すること。あるデータ管理者から他のデータ管理者への直接移行の場合において、トークンベースの認証などの委任による認証を使用すべきこと。

Such security measures must not be obstructive in nature and must not prevent users from exercising their rights, e.g. by imposing additional costs.
このような安全対策は、本質的に権利行使に対する妨害性となってはならず、また、例えば追加のコストを課すなどして、ユーザーの権利行使を妨げてはならない。

How to help users in securing the storage of their personal data in their own systems?
ユーザーが自己のシステムにおいて自己の個人データを安全に保管できるようどのように手助けするか？

By retrieving their personal data from an online service, there is always the risk that users may store them in less secured systems than the one provided by the service. The data subject requesting the data is responsible for identifying the right measures in order to secure personal data in his own system. However, he should be made aware of this in order to take steps to protect the information he has received. As an example of leading practice data controllers may also recommend appropriate format(s), encryption tools and other security measures to help the data subject in achieving this goal.
ユーザーは、オンラインサービスから自己の個人データを回収することにより、そのサービスで提供されたシステムよりも安全性が劣るシステムに自己の個人データを保存するおそれがある。データの要求をするデータ主体は、自己のシステムにおける個人データの安全性を確保するため、適切な方策を特定する責任がある。しかしながら、データ主体は、自己が受領した情報を保護するための措置を採るために、これを認識するようにされるべきである。そして、指導的な慣行の例として、データ主体がこの目的を達成できるよう、データ管理者が適切な形式、暗号化対策、及び他の安全対策を推奨することがありうる。

* * *

Done in Brussels, on 13 December 2016

For the Working Party,

The Chairwoman

Isabelle FALQUE-PIRROTIN

As last revised and adopted on 05 April 2017

For the Working Party,

The Chairwoman

Isabelle FALQUE-PIRROTIN