ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

16/EN

WP 242 rev.01

Guidelines on the right to data portability
關於資料可攜權之指引

Adopted on 13 December 2016

2016 年 12 月 13 日通過

As last Revised and adopted on 5 April 2017

2017 年 4 月 5 日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

由歐盟執委會司法與消費者總署C署（基本權利與法規）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 05/35號辦公室。

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

網址：http://ec.europa.eu/justice/data-protection/index_en.htm

TABLE OF CONTENTS 目錄

Executive summary

摘要

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條創造了一種新的資料可攜權，此權利與近用權密切相關，卻又在許多面向與之不同。可攜權允許當事人得以結構性、一般性和機器可讀性之格式接收其提供予控管者之個人資料，並將這些資料傳輸至另一資料控管者。此項新權利之目的係賦予當事人權利，並使其能更有效控制與自身相關之個人資料。

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.

由於資料可攜權允許將個人資料從一資料控管者直接傳輸至另一資料控管者，因此該權利亦是支持歐盟個人資料之自由流通和促進控管者競爭的重要工具。資料可攜權將增進不同服務提供商之間的轉換，從而促進在數位單一市場背景下開發新服務。

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.

本意見為GDPR中資料可攜權之解釋和執行方式提供了指導。其目的在於討論資料可攜權及其範圍。本意見闡明了此一新權利之適用條件，同時考量到資料運用的法律依據（當事人同意或為履行契約所必要）以及此權利僅適用於由當事人提供之個人資料的事實。本意見亦提供了具體之示例和標準來解釋該權利之適用情形。於此面向上，

29條工作小組認為資料可攜權涵蓋當事人有意識和積極提供之資料以及因當事人之行為而產生之個人資料。此項新權利不得被損害，且不限於當事人直接傳達之個人資訊，例如，線上表格。

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.
作為一種優良實務範例，資料控管者應開始建立有助於回應資料攜帶請求之方法，例如可供下載之工具和應用程式介面。控管者應確保個人資料以結構性、一般性和機器可讀性之格式傳輸，並應鼓勵其在執行資料攜帶請求時，須確保所提供資料格式之互通性。

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.
本意見亦有助於資料控管者清楚地瞭解各自之義務，並就支持遵守資料可攜權的優良實務範例和工具提供建議。最後，本意見建議產業相關者和同業公會在一套通用且可互通之標準和格式上協同作業，以實現資料可攜權之需求。

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

I. Introduction
導言

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.
一般資料保護規則（GDPR）第20條導入了新的資料可攜權。該權利允許當事人得以結構性、一般性和機器可讀性之格式接收其提供予控管者之個人資料，並不受妨礙地將這些資料傳輸至另一資料控管者。在符合特定要件下，此權利支持用戶選擇、用戶控制和用戶授權。

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).
過去個人依據第95/46/EC號資料保護指令行使近用權時，會受限於資料控管者在提供所請求資訊時所選擇之格式。**新的資料可攜權旨在賦予當事人關於自身個人資料之能力，該權利有助於當事人輕易地將個人資料從一個IT環境中移動、複製或傳輸至另一個IT環境**（無論是其本身之系統、可信任第三方之系統亦或其他新的資料控管者之系統）。

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].
透過確認當事人之個人權利和相關個人資料之控制，資料可攜性亦代表了一種機會，可「再平衡」當事人和資料控管者之間的關係[1]。

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].
雖然個人資料可攜權得增加服務間之競爭（透過促進服務轉換），但GDPR所規範的是個人資料而非競爭。尤其是，第20條並未將可攜資料限縮於為轉換服務所必需或有用之資料

[1] The primary aim of data portability is enhancing individual's control over their personal data and making sure they play an active role in the data ecosystem.
資料可攜性之主要目的係增強當事人對其個人資料之控制，並確保其在資料生態系統中扮演積極之角色。

[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.
雖然資料可攜權係一項新的權利，但其他類型之可攜性其實已存在或正在其他法律領域中進行討論（例如，在終止契約、通訊漫遊服務和跨境存取服務之背景下[3]）。在不同類型可攜性間，若以結合之方式提供可攜性，可能會出現對當事人的一些增效作用甚至益處，然類推適用時仍應謹慎。

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.
本意見為資料控管者提供指導，使控管者可更新其實務做法、程序和政策，並闡明資料可攜性之含義，使當事人得有效地行使此一新權利。

II. What are the main elements of data portability?
資料可攜性之主要要件為何？

The GDPR defines the right of data portability in Article 20 (1) as follows:
GDPR第20條第1項對資料可攜權之定義如下：

> *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 [...]*
> *當事人應有權利以結構性、一般性和機器可讀性之格式接收其提供予控管者與自身相關之個人資料，並有權利不受其提供個人資料之控管者妨礙，將這些資料傳輸至另一資料控管者[...]*

- **A right to receive personal data**

[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.
例如，該權利可在用戶的控制下，允許銀行使用當初因為能源供應服務而蒐集之個人資料以提供附加服務。
[3] See European Commission agenda for a digital single market: https://ec.europa.eu/digital-agenda/en/digital-single-market, in particular, the first policy pillar "Better online access to digital goods and services".
請參閱歐盟執委會關於數位單一市場之議程：https://ec.europa.eu/digital-agenda/en/digital-single-market，尤其是第一項政策支柱「更優質之網路數位商品和服務之存取」。

接收個人資料之權利

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.

首先，資料可攜性是一種**當事人接收**由資料控管者運用之相關**個人資料子集**，並為進一步個人使用而儲存這些資料**的權利**。此種儲存可在私人設備或私人雲端上，不一定需將資料傳輸至另一資料控管者。

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].

在此情形下，資料可攜性補充了近用權。資料可攜性的一個特點即在於為當事人提供了一種簡單的方式來管理和再使用個人資料。這些資料必須*以「結構性、一般性和機器可讀性之格式」接收*。例如，當事人可能有興趣從串流音樂服務中取得當前的播放列表（或收聽曲目的歷史紀錄），以找出特定曲目收聽次數，或用以比對在另一平台上想要購買或收聽的音樂。同樣的，當事人亦可能想從其網路郵件應用程式中取得聯絡人清單，例如為建立婚禮清單，抑或取得有關使用不同會員卡的購買資訊，或評估其碳足跡[4]。

- **A right to transmit personal data from one data controller to another data controller**

  將個人資料從一資料控管者傳輸至另一資料控管者之權利

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

[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.

在這些情形下，當所有運用皆係在當事人的單獨控制下所進行，由當事人對資料進行之運用可能落入家庭活動範圍，抑或在代表當事人之情況下，由另一方為之。若為後者之情形，該另一方應被視為資料控管者，即使僅用於個人資料之儲存，亦須遵守GDPR中規定之原則和義務。

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.

其次，第20條第1項規定當事人**有權利**「不受妨礙地」**將個人資料從一資料控管者傳輸至另一資料控管者**。在技術可行之情況下，依據當事人之請求，資料亦可直接從一資料控管者直接傳輸至另一資料控管者（第20條第2項）。於此面向，前言第68點鼓勵資料控管者建立互通之格式，以實現資料可攜性[5]，但不至課予控管者義務，要求採用或維護技術上相容之運用系統[6]。然而，GDPR確實禁止控管者設置傳輸障礙。

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.

基本上，此種資料可攜性之要素不僅為當事人提供了取得和再使用資料之能力，亦使其可就所提供之資料傳輸予另一服務提供商（無論是否在同一產業類別內）。除了透過賦予消費者權利以防止「被鎖在」某服務提供商，資料可攜權被預期可在當事人控制下，以安全可靠之方式促進創新及資料控管者間個人資料共享之機會[7]。資料可攜性可增進個人資料用戶在組織之間對個人資料在受控制的情形下進行有限之分享，從而豐富服務和客戶體驗[8]。在用戶感興趣的各種服務中，資料可攜性可促進相關用戶個人資料之傳輸和再使用。

- **Controllership**
  控制權

---

[5] See also section V.
請另參閱第V節。

[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.
因此，應特別注意傳輸資料之格式，以確保當事人或其他資料控管者可輕鬆地重複使用資料。請另參閱第V節。

[7] See several experimental applications in Europe, for example MiData in the United Kingdom, MesInfos / SelfData by FING in France.
請參閱歐洲各項實驗應用程式，例如英國的MiData，法國FING的MesInfos / SelfData。

[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.
所謂的自我量化和物聯網產業已經顯示出將個人資料與個人生活不同面向（如健身、活動和卡路里攝取）相互連結之益處（和風險），以便在單一檔案中提供更完整之個人生活描述。

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

資料可攜性確保當事人得依據其意願接收及運用個人資料之權利[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.

資料控管者在依據第20條規定之要件回應資料攜帶請求時，控管者不需對當事人或接收個資之另一家公司就該資料之運用負責。資料控管者代表當事人行事，包括將個人資料直接傳輸至另一資料控管者。在此情況下，考量到接收方並非傳輸資料之控管者所選擇，因此該資料控管者無法負責接收資料控管者對資料保護法之遵循。同時，控管者應設置安全維護措施，以確保其確實代表當事人行事。例如，控管者可建立程序以確保傳輸之個人資料類型確實為當事人所欲傳輸之資料。此程序可透過在傳輸前、在最初給予運用同意時、或於成立契約時獲得當事人之確認來完成。

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.

回應資料攜帶請求之資料控管者並無傳輸資料前檢查和驗證資料品質之特定義務。當然，依據GDPR第5條第1項規定之原則，這些資料應已是正確且最新的。此外，資料可攜性並未規定資料控管者有義務保留個人資料超過必要時間或超過任何指定的保留期限[10]。重要

[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.

資料可攜權不限於只針對與資料控管者提供類似服務之競爭者提供有用且相關之個人資料。

[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.

作為上述示例，若資料控管者並無保留用戶播放歌曲之記錄，則該個人資料不應包含在資料攜帶請求中。

的是，並未額外要求資料保留超出其所適用之保留期限，僅為提供任何未來可能之資料攜帶請求。

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.
若所請求之個人資料係由資料受託運用者所運用，依據GDPR第28條所簽訂之契約必須包括有義務「透過適當技術性和組織性措施協助控管者，（...）以回應當事人行使其權利之請求」。因此，資料控管者應與其資料受託運用者合作執行特定程序，以回應資料攜帶之請求。在共同控管之情況下，契約應明確分配各個資料控管者間關於處理資料攜帶請求之責任。

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.
此外，接收資料控管者[11]需負責確保被提供之可攜資料在新的資料運用上係相關且非過多的。例如，在向網路郵件服務者提出資料攜帶請求之情況下，當事人利用該請求以獲取電子郵件並將其發送至安全的歸檔備份平台，新的資料控管者不需運用當事人通訊聯絡人之詳細資訊。若此資訊與新的運用目的並無關聯，則不應保留和運用該資訊。在任何情況下，接收資料控管者並無義務接受和運用依資料攜帶請求傳輸過來之個人資料。同樣的，若當事人請求將其銀行交易之詳細資訊傳輸至提供協助管理財務之服務，一旦該資料為提供新

[11] i.e. that receives personal data following a data portability request made by the data subject to another data controller.
即依當事人資料攜帶請求接收個人資料之另一資料控管者。

服務之目的而標籤化，則接收資料控管者不需接受所有資料或保留所有交易詳細資訊。易言之，被接受和保留之資料應僅限於接收資料控管者為提供服務所必需和相關之資料。

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].

「接收」資料的組織成為這些個人資料之新資料控管者，且必須遵守GDPR第5條中規定之原則。因此，「新的」接收資料控管者必須依據第14條規定之透明化要求，在回應任何可攜資料傳輸請求前，清楚且直接地說明新的運用目的[12]。對於在其責任範圍內進行的任何其他資料運用，資料控管者應遵守第5條規定之原則，如合法性、公正性和透明化、目的限制性、資料最小化、準確性、完整性和機密性、儲存限制和課責性[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.

持有個人資料之資料控管者應就協助其當事人行使資料可攜權有所準備。資料控管者亦可選擇，但無義務，接受來自當事人之資料。

- **Data portability vs. other rights of data subjects**
  資料可攜性 vs. 當事人之其他權利

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

[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.
此外，新的資料控管者不得運用不相關之個人資料，且運用必須限於為新目的所必需，即使透過攜帶性程序傳輸之個人資料屬於更整體性資料集之一部分。非為實現新的運用目的所必需之個人資料應盡快刪除。

[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.
作為資料可攜權之一部分而被傳輸之個人資料，一旦被資料控管者接收，即可被視為「由當事人提供」。若適用於資料可攜權之其他法律要件（即運用之法律基礎，.....）得到滿足，並可依據資料可攜權再傳輸。

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.

當個人行使其資料可攜權時，此行為並不影響該當事人任何其他權利（如同GDPR中的任何其他權利）。即使在資料可攜性作業後，當事人亦可繼續使用資料控管者之服務並從中受益。資料可攜性不會自動觸發從資料控管者系統中移除資料[14]，亦不會影響適用於已傳輸資料之原始保存期。只要資料控管者仍繼續運用該資料，當事人即可行使其權利。

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.

同樣的，若當事人欲行使其刪除權（第17條規定之「被遺忘權」），資料控管者不得將資料可攜性作為延遲或拒絕此類刪除之方式。

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.

若當事人發現依據資料可攜權請求之個人資料未能完全滿足其請求時，依據GDPR第15條，當事人基於近用權所為之任何進一步個人資料請求皆須被完全遵從。

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.

此外，當某一特定歐盟或其成員國法律於其他領域中就相關資料亦提供了某種形式之可攜帶性，在滿足GDPR下之資料攜帶請求時，亦須考量這些特定法律規定之要件。一方面，若當事人之要求明確表示其意圖並非行使GDPR中之權利，而僅係依據某特定領域之法律行使權利，則GDPR的資料可攜性條款將不適用於該請求[15]。另一方面，若請求之目的係

[14] as stated in Article 17 of the GDPR
如GDPR第17條所述。

[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.
例如，若當事人之請求係針對向帳戶資訊服務提供商提供對其銀行帳戶過往記錄之存取，則基於支付服務指令2（PSD2）中所述之目的，應依據該指令之規定授予此類存取之權限。

針對GDPR下之可攜性，則此種特定法律之存在並不會優先於GDPR所規定的對任何資料控管者就資料可攜性原則之一般適用。相反的，必須依據具體情況逐案評估這些特定法律如何影響資料可攜性。

III. When does data portability apply?
何時適用資料可攜性？

- **Which processing operations are covered by the right to data portability?**
  資料可攜權涵蓋何種運用作業？

Compliance with the GDPR requires data controllers to have a clear legal basis for the processing of personal data.
GDPR合規性要求資料控管者須具有運用個人資料之明確法律基礎。

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:
依據GDPR第20條第1項第a款，**為落入資料可攜性之範圍內**，運用作業必須基於：

- 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);
  當事人之同意（依據第6條第1項第a款，或依據第9條第2項第a款，當涉及特殊類型之個人資料時）；

- or, on a contract to which the data subject is a party pursuant to Article 6(1)(b).
  或當事人為締約方之契約（依據第6條第1項第b款）。

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.
例如，當事人從網路書店所購買書籍之書名，或透過音樂串流媒體服務收聽之歌曲通常是在資料可攜性範圍內之個人資料示例，因其係基於履行當事人為締約方之契約所為之運用。

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.

當個人資料之運用非基於同意或契約之情況下，GDPR並未建立資料可攜性之一般權利[16]。例如，作為防止和偵查洗錢及其他金融犯罪義務之一部分所為之資料運用，金融機構並無義務回應有關此類個人資料之資料攜帶請求；同樣的，當運用既非基於當事人之同意，亦非基於當事人為契約締約方之情況下，資料可攜性不涵蓋企業對企業關係中所運用之職業聯絡明細。

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.

當涉及員工資料時，資料可攜權通常僅適用於基於當事人為締約方之契約的運用情形。在許多情況下，由於雇主和員工之間的權力不對等，同意將無法被視為係自由給予的[17]。某些人力資源之運用係基於正當利益之法律依據，或係為遵守就業領域中之特定法律義務所必需。實務上，人力資源背景下之資料可攜權無疑將涉及某些運用作業（例如薪資、補償服務和內部招聘），但在許多其他情況下，須以個案方式來驗證是否所有適用於資料可攜權之要件皆被滿足。

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，資料可攜權僅適用於當資料運用係「透過自動化方式執行」時，因此大多數的書面

---

[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).

請參閱GDPR前言第68點和第20條第3項。第20條第3項和前言第68點規定，資料可攜性不適用於當資料運用係為執行公共利益之任務或行使資料控管者被賦與之官方權限所必需時，抑或當資料控管者正在履行其公務職責或遵守法律義務。因此，在這些情況下，資料控管者並無義務提供可攜性。然而，透過遵守管理資料可攜權之原則，建立自動回應資料攜帶請求之程序是一種優良實務做法。此方面之示例為政府服務提供可輕鬆下載過去個人所得稅申報表。當運用之法律依據係基於正當利益和現有自願性計劃所必須時，資料可攜性之優良實務做法請參閱29條工作小組第6/2014號意見第47和48頁關於正當利益的部分（WP217）。

[17] As the WP29 outlined in its Opinion 8/2001 of 13 September 2001 (WP48).

如29條工作小組在2001年9月13日的第8/2001號意見（WP48）中所述。

檔案不涵蓋在內。

- **What personal data must be included?**
  必須包含何種個人資料？

Pursuant to Article 20(1), to be within the scope of the right to data portability, data must be:
根據第20條第1項，在資料可攜權範圍內，資料必須是：

- personal data concerning him or her, and
  與當事人相關之個人資料，及

- which he or she has *provided* to a data controller.
  由當事人*提供*予資料控管者之個人資料。

Article 20(4) also states that compliance with this right shall not adversely affect the rights and freedoms of others.
第20條第4項亦規定，對此一權利之遵守不得對他人之權利和自由產生不利影響。

First condition: personal data concerning the data subject
第一項要件：與當事人相關之個人資料

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.
僅有個人資料屬於資料攜帶請求之範圍內。因此，任何匿名[18]或與當事人無關之資料皆不在此範圍內。然而，可清楚與當事人連結之假名化資料（例如，由當事人提供相對應之識別資訊，請參閱第11條第2項）則屬於此範圍內。

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

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

would adversely affect the rights and freedoms of the third-parties (see below: third condition).
在許多情況下，資料控管者會運用包含數個當事人個人資料之資訊。在此情況下，資料控管者不應對「與當事人相關之個人資料」一詞採取過度限縮之解釋。例如，電話、個人間通訊或網路電話（VoIP）之記錄可包括（在用戶帳戶歷史中）來電或去電第三方之資訊細節。雖然該記錄包含相關數個當事人之個人資料，但用戶應仍能夠依資料攜帶請求取得這些記錄，因該記錄（亦）與該當事人相關。然而，若這些記錄隨後被傳輸至新的資料控管者，則新的資料控管者運用該資料之任何目的不得對第三方之權利和自由產生不利影響（請參閱下文：第三項要件）。

Second condition: data provided by the data subject
第二項要件：由當事人提供之資料

The second condition narrows the scope to data "provided by" the data subject.
第二項要件將範圍限縮至由當事人「提供」之資料。

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.
有許多個人資料係由當事人有意識且積極「提供」之示例，例如透過網路表格提交之帳戶資料（例如郵件地址、用戶名稱、年齡）。然而，觀察其活動所得之資料亦屬由當事人「提供」之資料。因此，29條工作小組認為，為充分發揮此項新權利之價值，「提供」亦應包括從用戶活動中觀察到的個人資料，如智慧型電錶所運用之原始資料或其他類型之連結物件[19]、活動日誌、網站使用或搜尋活動的歷史記錄。

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.
後者資料種類不包括由資料控管者創建之資料（使用觀察到或直接輸入提供之資料），例如透過分析所蒐集之原始智慧型電錶資料而創建之用戶檔案。

A distinction can be made between different categories of data, depending on their origin, to

[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.
透過取得觀察其活動所產生之資料，當事人亦將能夠更佳地了解資料控管者對觀察資料範圍之執行選擇，並將處於更佳之地位選擇願意提供何種資料以獲得類似之服務，且可了解其隱私權在何種程度上受到尊重。

determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":
依據其來源可區分為不同類型之資料，從而確認其是否屬於資料可攜權之範圍。以下資料類型可被視為「由當事人提供」：

- **Data actively and knowingly provided by the data subject** (for example, mailing address, user name, age, etc.)
  當事人積極且有意識提供之資料（例如郵件地址、用戶名稱、年齡等）

- **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.
  經由使用服務或設備而由當事人提供之觀察資料。此類型資料可包括例如個人搜尋歷史、流量資料和位置資料。其亦可包括其他原始資料，例如由穿戴式裝置所追蹤之心跳。

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].
相反者為由資料控管者基於「由當事人提供」之資料所創建之推論資料和衍生資料。例如，關於用戶健康狀況評估之結果，或在風險管理和財務法規背景下創建之檔案（例如，給予信用評分或遵守反洗錢法規）不得被視為由當事人「所提供」。即使此類資料可能係資料控管者所存留檔案之一部分，並且係透過當事人所提供之資料分析推論或衍生而來（例如透過當事人之行為），這些資料通常不會被視為「由當事人提供」，因此不屬於此項新權利之範圍[20]。

[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).
然而，當事人仍可行使其「從控管者取得關於是否正在運用與當事人相關個人資料之確認的權利，並且在這種情況下，得近用個人資料」，以及關於「第 22 條第 1 項和第 4 項所提及自動化決策 （包含剖析）之存在，以及至少於這些情況下，依據 GDPR 第 15 條（涉及近用權）規定，取得關於所涉邏輯，以及這些資料之運用會對當事人造成之重大和預計之後果之有意義資訊」。

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].

一般而言，鑑於資料可攜權之政策目的，「由當事人提供」一詞必須做廣義之解釋，並應排除「推論資料」和「衍生資料」，此包括由服務提供者創建之個人資料（例如，演算法之結果）。資料控管者可排除這些推論資料，但應包含當事人透過控管者所提供之技術方式而提供的所有其他個人資料[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.

因此，「由...提供」一詞包括與當事人活動相關之個人資料或由觀察個人行為所得之結果，但不包括由該行為之後續分析產生之資料。相反的，任何由資料控管者作為資料運用之一部分而創建的個人資料（例如透過個人化或推薦程序、透過用戶分類或剖析），是由當事人提供之個人資料衍生或推論而來，並不屬於資料可攜權之範圍。

Third condition: the right to data portability shall not adversely affect the rights and freedoms of others

第三項要件：資料可攜權不應對他人之權利和自由產生不利影響

With respect to personal data concerning other data subjects:

與其他當事人相關之個人資料：

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].

[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.

此包括基於資料蒐集目的，在活動期間觀察到與當事人相關之所有資料，例如交易歷史或存取記錄。透過追蹤和記錄當事人而蒐集之資料（例如記錄心跳之應用程式或用於追蹤瀏覽行為之技術）亦應被視為「由當事人所提供」，即使該資料並非是被積極或有意識地傳輸。

第三項要件旨在避免取得和傳輸包含其他（未經同意）當事人之個人資料至新的資料控管者，當這些資料之運用方式可能會對該其他當事人之權利和自由產生不利影響（GDPR第20條第4項）[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.).
例如，若從一資料控管者向另一資料控管者傳輸資料，將會阻止第三方行使其作為GDPR下當事人之權利（例如被告知權、近用權等）時，則會產生此種不利影響。

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.
當事人經由給予新的資料控管者同意，或與該控管者簽訂契約，而開始傳輸其個人資料至另一資料控管者。若資料集包含第三方之個人資料，則必須確認資料運用的另一法律依據。例如，資料控管者可依據第6條第1項第f款尋求正當利益，尤其是當資料控管者之目的係向當事人提供服務，而該服務允許後者為純粹的個人或家庭活動運用個人資料。在涉及並可能影響第三方的個人活動環境中，若資料控管者無法以任何方式決定此種運用，則此由當事人發起之運用作業仍應由該當事人負責。

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.
例如，網路郵件服務可允許當事人建立其聯絡人、朋友、親戚、家庭和更廣泛情況之目錄。由於這些資料與希望行使資料可攜權之可識別當事人相關（並由其建立），資料控管者應

[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."
前言第68點規定「在某些個人資料集內，當涉及數個當事人之情況下，接收個人資料之權利不應影響其他當事人依據本規則享有之權利和自由。」

將接收和傳送電子郵件的完整目錄傳輸予該當事人。

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.

同樣的，當事人之銀行帳戶可包含涉及帳戶持有人以及與其他當事人相關之個人交易資料（例如，若其他當事人將金錢轉帳予帳戶持有人）。若帳戶持有人提出攜帶請求將銀行帳戶資訊傳輸予其本人，則不大可能對這些第三方之權利和自由產生不利影響 – 因在此兩個示例中，資料皆用於相同之目的（即僅由當事人使用之聯絡地址或當事人銀行帳戶的歷史紀錄。）

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.

相反的，若新的資料控管者將個人資料用於其他目的時，第三方之權利和自由將沒有受到尊重。例如，若接收資料控管者基於行銷目的使用當事人聯絡目錄中其他當事人之個人資料。

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.

因此，為防止對相關之第三方產生不利影響，僅有當資料係由用戶單獨控制且僅係針對個人或家庭需求進行管理時，始允許由另一資料控管者運用此類型之個人資料。接收資料之「新的」資料控管者（依用戶請求向其傳輸資料）不可將所傳輸之第三方資料用於其自身

之目的，例如向其他第三方當事人提供貨品或服務行銷。例如，在未經第三方當事人知情和同意之情況下，此資訊不應用於充實其檔案和重建其社交環境[23]。即便資料控管者已持有其個人資料，此資訊亦不得用於取得有關該第三方之資訊並用來創建特定檔案。否則，此種運用可能係非法且不公平，特別是若相關之第三方並未被告知且無法行使其作為當事人之權利時。

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.
此外，作爲優良實務做法，所有資料控管者（「傳輸」和「接收」方）都應建置工具使當事人得選擇其所希望接收和傳輸之相關資料，並在適當時排除其他當事人之資料。如此將進一步協助降低第三方個人資料可能被輸出之風險。

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.
此外，資料控管者應為相關之其他當事人建置同意機制，以便在該當事人願意提供同意之情況下更容易為資料傳輸，例如若該當事人亦欲將其資料轉移至其他資料控管者。比方，社群網路就可能會出現此種情況，但遵循何種實務作法，由資料控管者決定。

With respect to data covered by intellectual property and trade secrets:
關於智慧財產和營業秘密所涵蓋之資料：

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).
第20條第4項提及了他人之權利和自由。雖然與可攜性並無直接關聯，但此可理解為「包含營業秘密或智慧財產權，尤其係保護軟體之著作權」。然而，即使在回應資料攜帶請求

[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.
若無法尊重透明化原則並確保特定運用係基於適當法律依據，社群網路服務不應透過使用當事人行使其資料可攜權而傳輸之個人資料以充實其會員檔案。

之前應考量這些權利，「不得以考量之結果拒絕向當事人提供所有資訊」。此外，資料控管者不應基於侵害另一契約權利（例如未清償債務或與當事人之交易衝突）拒絕資料攜帶之請求。

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.
當資訊之使用方式可能被視為不公平，或構成對智慧財產權之侵犯時，資料可攜權即非當事人得濫用資訊之權利。

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.
然而，潛在之商業風險本身不可作為拒絕回應資料攜帶請求之基礎，且資料控管者得以不洩露營業秘密或智慧財產權資訊之形式傳輸由當事人提供之個人資料。

IV. How do the general rules governing the exercise of data subject rights apply to data portability?
規範行使當事人權利之一般規則如何適用於資料可攜性？

- **What prior information should be provided to the data subject?**
  應向當事人提供何種前置資訊？

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).
為符合新的資料可攜權，資料控管者必須告知當事人此項新的資料可攜權之存在。若直接從當事人處蒐集相關之個人資料，則必須「在獲得個人資料時」告知。若非從當事人處獲得個人資料，則資料控管者必須提供第13條第2項第b款和14條第2項第c款要求之資訊。

"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].
「若非從當事人處獲得個人資料」，第14條第3項規定資訊必須在下列情況下提供：獲得

資料後之一個月內的合理時間、在與當事人進行首次溝通時、或在向第三方揭露時[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.
在提供所需資訊時，資料控管者必須確保其將資料可攜權與其他權利有所區分。因此， 29條工作小組特別建議資料控管者清楚地解釋，當事人透過近用權和資料可攜權得接收之資料類型間之差異。

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.
此外，工作小組也建議資料控管者在當事人關閉其可能擁有之任何帳戶前，提供包含有關資料可攜權之資訊。如此將允許用戶盤點評估其個人資料，並在契約終止前可輕鬆地將資料傳輸至自身之裝置或另一個提供者。

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，作為「接收」資料控管者的主要實務做法，29條工作小組建議向當事人提供與執行服務相關個人資料性質的完整資訊。除了加強公平運用之基礎外，此做法亦限縮用戶造成對第三方之風險，以及任何其他非必要個人資料之複製，即使該複製並未涉及其他當事人。

- **How can the data controller identify the data subject before answering his request?**
  在回應請求前，資料控管者如何識別當事人？

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

[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條規定資料控管者提供之「任何溝通[…]需以簡明、透明、易懂和易於評估之形式為之並使用清晰簡潔之語言，尤其係專門針對兒童之任何資訊。」

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.

在GDPR中並無關於如何認證當事人之法定要求。然而，GDPR第12條第2項規定，除非控管者運用個人資料之目的不需識別當事人，且其可證明無法識別該當事人，否則資料控管者不得拒絕當事人行使其權利（包括資料可攜權）之請求。然而，依據第11條第2項，在此種情況下，當事人可提供更多資訊以便識別其身分。此外，第12條第6項規定，若資料控管者對當事人身分有合理的懷疑時，可要求提供進一步資訊以確認當事人身分。若當事人提供得識別其身分之額外資訊時，資料控管者不得拒絕對該請求採取行動。當線上蒐集之資訊和資料與假名化或特殊標識相連結時，資料控管者即可執行適當程序，以使當事人能夠提出資料攜帶請求並接收與其相關之資料。無論如何，資料控管者必須執行認證程序，以加強確認請求其個人資料或一般性行使GDPR權利之當事人身分。

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].

這些程序通常已經存在。在與其簽訂契約或取得對運用之同意前，資料控管者通常已對當事人進行了認證。因此，用於註冊之與運用相關的當事人個人資料亦可做為證據，以便為可攜性之目的驗證當事人[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 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

[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.
例如，當資料運用連結至用戶帳戶時，提供相關之登錄名稱和密碼可能足以識別當事人。

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.
雖然在這些情況下，當事人事前之身分識別可能需要請求其提供合法身分證明，但這種認證可能與評估資料和相關個人間之連結性無關，因為此類連結性與正式或合法身分並無關聯。基本上，資料控管者請求額外資訊以評估當事人身分之能力，不得導致過多之要求，和導致蒐集與強化個人和所請求個人資料間之連結無關或不必要之個人資料。

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.
在許多情況下，此種認證程序已經存在。例如，用戶名稱和密碼通常用於允許當事人存取其電子郵件帳戶、社群網路帳戶和用於各種其他服務之帳戶，而對於某些帳戶之使用，當事人會選擇不透露其全名和身分。

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).
若當事人請求之資料大小在使用網路傳輸時會造成問題，資料控管者與其可能容許最長三個月的延長期限以遵循請求[26]，不如考量以替代方式提供資料，例如使用串流傳輸或儲存到CD、DVD或其他實體媒介，或允許個人資料直接傳輸至另一資料控管者（依據GDPR第20條第2項當技術可行時）。

- **What is the time limit imposed to answer a portability request?**
  回應可攜性請求之時間限制為何？

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條第3項要求資料控管者向當事人「告知所欲採取之行動」，「不得無故延遲」，且

[26] Article 12(3): "The controller shall provide information on action taken on a request".
第12條第3項：「控管者應提供對請求所欲採取行動之資訊」。

無論如何，「在收到請求後的一個月內」為之。對於複雜案件，此一個月之期限最多可延長至三個月，前提是當事人已於原始請求的一個月內被告知此類延遲之原因。

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.
經營資訊社群服務之資料控管者可能有較佳之能力，能夠在很短的時間內遵循請求。為了滿足用戶的期待，明確界定通常可回應資料攜帶請求之時間範圍，並將其傳達予當事人，為優良實務做法。

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.
拒絕回應攜帶請求之資料控管者應依據第12條第4項，於收到請求後的一個月內，通知當事人「不採取行動之原因以及可向監管機關提出申訴和尋求司法救濟之可能性」。

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.
資料控管者必須尊重在規定時間內作出回應之義務，即便是拒絕。易言之，當資料控管者被要求就資料攜帶請求做出回應時，不得保持沉默。

- **In which cases can a data portability request be rejected or a fee charged?**
  於何種情況下可拒絕資料攜帶的請求或收取費用？

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條禁止資料控管者為提供個人資料收取費用，除非資料控管者得證明請求明顯無依據或過度，「尤其是因為具有重複性」。對於擅長於自動化運用個人資料之資訊社群服務，執行諸如應用程式介面（API）[27]之類的自動化系統可促進與當事人間之交換，因而減少

[27] Application Programming Interface (API) means the interfaces of applications or web services made available

了因重複請求導致的潛在負擔。因此，即使對於多個資料攜帶請求，資料控管者極少能夠證明拒絕提供請求資訊有正當理由。

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.
此外，為回應資料攜帶請求而建立之程序總成本不應在決定請求是否過度時列為考量。事實上，GDPR第12條係針對單一當事人所提出之請求，而非資料控管者收到的請求總數量。因此，整體系統執行成本既不應向當事人收取費用，亦不應用於證明拒絕回應可攜性請求具有正當理由。

V. How must the portable data be provided?
如何提供可攜資料？

- What are the expected means the data controller should implement for data provision?
資料控管者為提供資料所應執行之預期方式為何?

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條第1項規定，當事人有權利將資料傳輸至另一控管者，而不受其提供個人資料之控管者所阻礙。

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].
此種阻礙可表徵為資料控管者為阻止或減慢當事人或其他資料控管者之存取、傳輸或再使用而設置之任何法律、技術或財務障礙。例如，此種阻礙可能為：要求傳輸資料之費用、缺乏資料格式或API或所提供格式之互通性或可存取性、取得完整資料集之過度延遲或複

by data controllers so that other systems or applications can link and work with their systems.
應用程式介面（API）係指資料控管者提供之應用程式或網頁服務介面，以便其他系統或應用程式可連結和使用其系統。

雜性、故意模糊資料集、或特殊和不當或過度的產業標準化或認證要求[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條第2項亦規定了資料控管者「在技術上可行時」有直接將可攜資料傳輸予其他資料控管者之義務。

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".
在當事人控制下，從一資料控管者傳輸至另一資料控管者之技術可行性，應依據個案具體情況進行評估。前言第68點進一步闡明「技術上可行」之限制，並指出「不應要求控管者有義務採行或維護技術上相容之運用系統」。

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)).
資料控管者被期待能以可互通之格式傳輸個人資料，即便其他資料控管者並未被課以支援這些格式之義務。因此，當兩個系統之間的安全通訊[29]為可行，以及當接收系統在技術上處於可接收輸入資料之狀態，即可將資料從一資料控管者直接傳輸至另一資料控管者。若因技術障礙禁止直接傳輸，資料控管者應向當事人解釋這些障礙，否則將與拒絕依當事人請求採取行動的決定相類似（第12條第4項）。

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:
在技術性層面上，為了對當事人或其他資料控管者提供可攜資料，資料控管者應研究和評估兩種不同且互補之方式：

[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).
某些合法障礙可能存在，如與第 20 條第 4 項中所提及他人之權利和自由相關之障礙，或與控管者自身系統安全相關之障礙。資料控管者有責任證明為何這些障礙係合法的，以及為何不構成第 20 條第 1 項中之阻礙。
[29] Through an authenticated communication with the necessary level of data encryption.
透過具有必要等級資料加密之驗證通訊。

- a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset);
  直接傳輸可攜資料之整體資料集（或全部資料集之數項摘錄）；

- an automated tool that allows extraction of relevant data.
  允許提取相關資料之自動化工具。

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.
在涉及複雜和大量資料集之情況下，資料控管者可能傾向選擇第二種方式，因該方式允許當事人在其請求之背景下，提取與其相關資料集之任何部分，且有助於風險最小化，並可能允許使用資料同步機制[30]（例如，在資料控管者間正常之通訊情境下）。此方式可能是確保「新的」資料控管者合規性的較佳方式，且在原始資料控管者方面，可做為降低隱私風險之優良實務做法。

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.
為提供相關可攜資料，這兩種不同且可能互補之方式得透過各種方式執行以取得資料，例如，安全訊息傳遞、SFTP伺服器、安全WebAPI或WebPortal。應使當事人能夠利用個人資料儲存、個人資訊管理系統[31]或其他類型可信任之第三方，以持有和儲存個人資料，並授權資料控管者依據請求存取和運用個人資料。

- **<u>What is the expected data format?</u>**

[30] Synchronisation mechanism can help reaching the general obligations under Article 5 obligation of the GDPR, which provides that "personal data shall be (…) accurate and, where necessary, kept up to date"
同步機制有助於實現 GDPR 第 5 條義務下之一般義務，該條款規定「個人資料應(…)準確，且在必要時隨時更新」。

[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
有關個人資訊管理系統（PIMS），請參閱，例如EDPS第9/2016號意見：https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

預期之資料格式為何？

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要求資料控管者以支援再使用之格式提供當事人所請求之個人資料。具體而言，GDPR第20條第1項規定，個人資料必須「以結構性、一般性和機器可讀性之格式」提供。前言第68點進一步闡釋了此種格式應可互通，互通一詞在歐盟被定義為[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.*
> *有能力使迥然不同且多樣化之組織能夠藉由各自 ICT 系統之間的資料交換，透過其支援之業務程序，實現互利之共同目標，包括在各組織之間共享資訊和知識。*

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, "structured, commonly used and machine readable" are specifications for the means, whereas interoperability is the desired outcome.

「結構性」、「一般性」和「機器可讀性」係促進資料控管者提供可互通資料格式之最低要求。也就是說，「結構性、一般性和機器可讀性」係就方法之描述，而互通性係所預期之結果。

Recital 21 of Directive 2013/37/EU[33,34] defines "machine readable" as:

第2013/37/EU號指令前言第21點[33,34]將「機器可讀性」定義為：

> *a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal*

---

[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.
歐洲議會和理事會 2009 年 9 月 16 日第 922/2009/EC 號決議第 2 條，關於歐洲公共行政部門（ISA）之互通性解決方案 OJ L 260,03.10.2009，p.20。

[33] Amending Directive 2003/98/EC on the re-use of public sector information.
修訂第2003/98/EC號指令關於重複使用公眾部門資訊。

[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*.
歐盟術語表（http://eur-lex.europa.eu/eli-register/glossary.html）進一步闡明了與本指引中所使用概念相關之期待，例如*機器可讀性、互通性、開放格式、標準、詮釋資料*。

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.
使軟體應用程式可輕易識別、辨認和提取特定資料之結構化檔案格式，包括個別描述及其內部結構。以機器可讀之結構化格式編碼之檔案資料為機器可讀式資料。機器可讀格式可以是開放或專有的；且可以是正式或非正式的標準。以限制自動運用之文件格式編碼的檔案，因不得或不易從中提取資料，所以不應視為係機器可讀格式。成員國應酌情鼓勵使用開放、機器可讀之格式。

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 large degree of data portability. As such, formats that are subject to costly licensing constraints would not be considered an adequate approach.
鑑於資料控管者潛在可運用的資料類型廣泛，GDPR並未對所需提供之個人資料格式提出具體建議。最合適之格式在不同產業之間亦會有所不同，且可能已有適當之格式存在，被選擇之格式應可達到得解釋之目的，並可為當事人提供很大程度之資料可攜性。因此，受到昂貴授權限制之格式將不被視為是適當之方式。

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].
前言第68點闡釋「當事人傳輸或接收有關其個人資料之權利不應加諸控管者義務，去採行或維護技術上相容之運用系統。」**因此，可攜性之目的在產生可互通之系統，而非相容之系統**[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

[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 定義互通性如下：「可在各種功能單元間溝通、執行程序或傳輸資料之能力，且要求用戶僅須稍微或不須了解這些單元之獨特性質。」

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.

提供個人資料之格式預期將以具高度抽象性的任何內部或專有格式為之。因此，資料可攜性意味著資料控管者另一層面的資料運用，以便從其平台提取資料並過濾可攜性範圍外之個人資料，例如推論資料或與系統安全性相關之資料。因此，鼓勵資料控管者事先識別其自身系統中可攜性範圍內之資料。此種額外的資料運用將被視為係主要資料運用之輔助運用，因其執行並非為達到資料控管者所定義之新目的。

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 re- used. 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.

若在特定行業或特定環境中並無一般性之使用格式，**資料控管者在提供資料時應使用常用的開放性格式（例如XML，JSON，CSV，...）以及有用且可達到最佳區別性之詮釋資料(metadata)**，同時保持高度抽象性。因此，應使用合適的詮釋資料，以便準確地描述所交換資訊之含義。此詮釋資料應可使資料具功能性且可再使用，但當然不至洩露商業機密。因此，為個人提供電子郵件收件匣的PDF版本資料不太可能具有足夠的結構性或描述性，使收件匣之資料可輕易地再使用。相反的，應以保留所有詮釋資料之格式提供電子郵件資料，以便有效地再使用資料。因此，在選擇提供個人資料的資料格式時，資料控管者應考量該格式將如何影響或阻礙當事人再使用資料之權利。若資料控管者能夠提供當事人選擇其偏好之個人資料格式，亦應對選擇之影響提供清楚的解釋。然而，當運用額外詮釋資料之唯一目的係該額外詮釋資料可能會被需要以回應資料攜帶請求，此即非該運用之正當依

據。

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].

29條工作小組強烈鼓勵產業相關人員和同業公會在一套通用且可互通之標準和格式上協同作業，以符合資料可攜權之要求。歐洲互通框架（EIF）亦對此挑戰提出解決方案，為那些希望共同提供公共服務的組織建立了一套議定的互通方法。在其適用範圍內，該框架規定了一系列之一般要件，例如詞彙、概念、原則、政策、指引、建議、標準、規格和實務做法[36]。

- **How to deal with a large or complex personal data collection?**
  如何處理大量或複雜之個人資料蒐集？

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.

當大量資料之蒐集、複雜資料結構或其他技術性問題可能對資料控管者或當事人造成困難時，GDPR並未解釋如何解決就此種挑戰之因應方式。

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.

然而，在所有情況下，當事人能夠完全理解資料控管者所提供個人資料之定義、概要和結

[36] Source : http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.
資料來源：http：//ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

構是至關重要的。例如，可先使用儀表板式的摘要形式提供資料，允許當事人可接收個人資料子集，而非整體資料。資料控管者應以「簡潔、透明、易懂且便於取得之形式，使用清晰、平易的語言文字」（請參閱GDPR第12條第1項）提供概述，使當事人可就既定目的而欲下載或傳輸至另一資料控管者之資料擁有明確資訊。例如，當事人應能夠使用軟體應用程式輕鬆識別、辨認和運用來自該程式之特定資料。

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.

如上所述，資料控管者可回應資料攜帶請求之實務作法，可以是提供適當受保護且經記錄建檔之API。誠如GDPR第20條第2項所述，如此可使當事人能夠透過其自身或第三方軟體向資料控管者請求個人資料，或授權他人代表其為之（包括另一資料控管者）。透過外部可存取之API授予對資料的近用權限，亦可能提供更複雜的存取系統，使當事人能夠為完整下載或僅為包含自上次下載以來變更之增量函數進行後續資料請求，而不因該額外請求造成對資料控管者之負擔。

-How can portable data be secured?

如何保護可攜資料？

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.

一般而言，資料控管者應依據GDPR第5條第1項第f款之規定，確保「適當的個人資料安全，並使用適當技術性或組織性措施，防止包括未經授權或非法運用，以及防止意外遺失、破壞或損毀」。

However, the transmission of personal data to the data subject may also raise some security issues:

然而，將個人資料傳輸予當事人亦可能會引發某些安全疑慮：

How can data controllers ensure that personal data are securely delivered to the right person?

資料控管者如何確保個人資料安全地傳輸予合適之人？

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.

由於資料可攜性之目的係從資料控管者之資訊系統中獲取個人資料，因此傳輸成為這些相關資料之可能風險來源（尤其是在傳輸期間之資料侵害）。資料控管者有責任採取所有必要的安全措施，不僅須確保安全地傳輸個人資料（透過使用端對端或資料加密）至正確目的地（透過使用強力認證措施），亦須繼續保護仍存留於其系統中之個人資料，以及確保能因應潛在資料侵害的透明程序[37]。因此，資料控管者應評估與資料可攜性相關之特定風險，並採取適當之降低風險措施。

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.

此類降低風險措施可包括：若當事人已需進行身分驗證，則使用附加的身分驗證資訊（如共用密碼）或其他身分驗證元素（如一次性密碼）；若懷疑帳戶已被盜用，則暫停或凍結傳輸；在從資料控管者直接傳輸至另一資料控管者之情況下，應強制使用授權驗證，例如token-based驗證。

Such security measures must not be obstructive in nature and must not prevent users from exercising their rights, e.g. by imposing additional costs.

此類安全措施不得具有阻礙性，不得防止用戶行使其權利，例如：透過收取額外費用。

How to help users in securing the storage of their personal data in their own systems?

如何協助用戶確保在其自身系統中所儲存個人資料之安全性？

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

[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.
符合第2016/1148號指令（EU）關於整體歐盟網路和資訊系統高度共同安全保護措施。

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.

透過網路服務取得個人資料，用戶難免有可能將其資料儲存於比較不安全（相較於服務所提供之系統）的系統中之風險。請求資料之當事人為了確保個人資料於其自身之系統中之安全，有責任識別正確之措施。然而，該當事人必須能瞭解到此情況，以便採取措施保護接收之資訊。作為主要實務示例，資料控管者亦可推薦適當之格式、加密工具和其他安全措施，以協助當事人實現此目標。

* * *

Done in Brussels, on 13 December 2016

2016年12月13日於布魯塞爾完成

For the Working Party,

工作小組

The Chairwoman

主席

Isabelle FALQUE-PIERROTIN

As last revised and adopted on 05 April 2017

2017年4月5日最後修訂並通過

For the Working Party

工作小組

The Chairwoman

主席

Isabelle FALQUE- PIERROTIN