ARTICLE 29 DATA PROTECTION WORKING PARTY
第29條個資保護工作小組

17/EN
WP260 rev.01

Article 29 Working Party
第29條個資保護工作小組
Guidelines on transparency under Regulation 2016/679
關於第2016/679號規則(GDPR)中的透明化之指引

Adopted on 29 November 2017

As last Revised and Adopted on 11 April 2018

2017年11月29日通過

2018年4月11日最後修訂並通過

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

關於個人資料運用*之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日通過之95/46/EC指令而設立，

基於該指令第29條及第30條，

基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:

通過此份指引：

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 Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
由歐盟執委會司法總署C署（基本權利與歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 02/013號辦公室。

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item type=1358&tpa id=6936
網址：http://ec.europa.eu/justice/data-protection/index_en.htm

*註釋：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」。

Table of Content 目錄

Introduction

導言

1. These guidelines provide practical guidance and interpretative assistance from the Article 29 Working Party (WP29) on the new obligation of transparency concerning the processing of personal data under the General Data Protection Regulation[1] (the "**GDPR**"). Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights[2]. Insofar as compliance with transparency is required in relation to data processing under Directive (EU) 2016/680[3], these guidelines also apply to the interpretation of that principle.[4] These guidelines are, like all WP29 guidelines, intended to be generally applicable and relevant to controllers irrespective of the sectoral, industry or regulatory specifications particular to any given data controller. As such, these guidelines cannot address the nuances and many variables which may arise in the context of the transparency obligations of a specific sector, industry or regulated area. However, these guidelines are intended to enable controllers to understand, at a high level, WP29's interpretation of what the transparency obligations entail in practice and to indicate the approach which WP29 considers controllers should take to being transparent while embedding fairness and accountability into their transparency measures.

   本指引係29條工作小組（WP29）依據一般資料保護規則（**GDPR**）[1]中就運用個人資料新設的透明化義務提供實務指導和解釋性協助。透明化是GDPR下的總體義務，且適用於三項主要領域：（1）向當事人提供公正運用之相關資訊；（2）資料控管者如何與當事人就其在GDPR下之權利進行溝通；以及（3）資料控管者如何使當事人便於行使其權利[2]。為遵循(EU)第2016/680號指令[3]下關於資料運用之透明化要求，本指引亦適用於該原

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
2016年4月27日歐洲議會與歐盟理事會在個人資料運用下為保護自然人與確保該資料之自由流通，制定（EU）第2016/679號規則，並廢除95/46 / EC指令。

[2] These guidelines set out general principles in relation to the exercise of data subjects' rights rather than considering specific modalities for each of the individual data subject rights under the GDPR.
這些指引規定有關當事人行使權利之一般原則，而非考量GDPR下每個當事人權利之特定模式。

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
2016年4月27日歐洲議會與歐盟理事會通過之（EU）第2016/680號指令，係關於權責機關為預防、調查、偵查或起訴犯罪或執行刑事處罰而運用個人資料及此類資料自由流通等情事之自然人保護，並廢除第2008/977 / JHA號理事會架構決定。

則之解釋[4]。與所有WP29指引相同，本指引旨在規範與控管者相關之普遍適用情形，而非考量任何特定資料控管者之行業、產業或監管規範。因此，本指引無法就特定行業、產業或受監管領域之透明化義務提出可能的細微差別和各種變數。然而，本指引目的在使控管者能夠高度理解WP29對透明化義務在實務應用上之解釋，並表明WP29認為控管者為符合透明化所應採取之方式，並同時將公正性和課責性納入其透明化措施。

2. Transparency is a long established feature of the law of the EU[5]. It is about engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes. It is also an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union. Under the GDPR (Article 5(1)(a)[6]), in addition to the requirements that data must be processed lawfully and fairly, transparency is now included as a fundamental aspect of these principles.[7] Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject.[8] Connected to this, the accountability principle requires transparency of processing operations in order that data controllers are able to demonstrate compliance with their obligations under the GDPR[9].

透明化是歐盟法律長期以來所建立之特點[5]，目的在於藉由使公民瞭解，或在必要時挑戰影響其權益之程序，從而使公民對該程序產生信任。透明化亦為歐盟基本權利憲章第8條所述關於個人資料運用之公正原則之展現。GDPR（第5條第1項第a款[6]）除了要求必須合法並公正地運用資料外，現在亦將透明化納入這些原則之基本方向[7]。透明化與公正性以及GDPR下新的課責性原則具有緊密關聯。且依據第5條第2項，控管者必須能夠證明

---

[4] While transparency is not one of the principles relating to processing of personal data set out in Article 4 of Directive (EU) 2016/680, Recital 26 states that any processing of personal data must be "lawful, fair and transparent" in relation to the natural persons concerned.
雖然透明化並非（EU）第2016/680號指令第4條關於運用個人資料的原則之一，但前言第26點指出，任何與自然人相關之個人資料運用必須是「合法、公正以及透明」的。

[5] Article 1 of the TEU refers to decisions being taken "*as openly as possible and as close to the citizen as possible*"; Article 11(2) states that "*The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society";* and Article 15 of the TFEU refers amongst other things to citizens of the Union having a right of access to documents of Union institutions, bodies, offices and agencies and the requirements of those Union institutions, bodies, offices and agencies to ensure that their proceedings are transparent.
歐洲聯盟條約（TEU）第1條規定決定之做成「*應盡可能公開且盡可能貼近公民*」；第11條第2項規定「*各機關應與協會代表和公民社會保持公開、透明和定期之溝通*」；以及歐洲聯盟運作條約（TFEU）第15條除其他事項外，規定歐盟公民有權查閱歐盟機關、機構、辦事處和局處之文件並要求該歐盟機關、機構、辦事處和局處確保其程序之透明。

[6] "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".
「與當事人相關之個人資料運用應以合法、公正和透明之方式為之」。

[7] In Directive 95/46/EC, transparency was only alluded to in Recital 38 by way of a requirement for processing of data to be fair, but not expressly referenced in the equivalent Article 6(1)(a).
在95/46 / EC指令中，透明化僅在前言第38點中藉由要求資料運用必須公正而間接提及，但並未在相應的第6條第1項第a款中敘明。

與當事人相關個人資料之運用是以透明的方式為之[8]。與此相關者，課責性原則要求運用作業之透明化，以便資料控管者得以證明其遵循GDPR規定之義務[9]。

3. In accordance with Recital 171 of the GDPR, where processing is already under way prior to 25 May 2018, a data controller should ensure that it is compliant with its transparency obligations as of 25 May 2018 (along with all other obligations under the GDPR). This means that prior to 25 May 2018, data controllers should revisit all information provided to data subjects on processing of their personal data (for example in privacy statements/ notices etc.) to ensure that they adhere to the requirements in relation to transparency which are discussed in these guidelines. Where changes or additions are made to such information, controllers should make it clear to data subjects that these changes have been effected in order to comply with the GDPR. WP29 recommends that such changes or additions be actively brought to the attention of data subjects but at a minimum controllers should make this information publically available (e.g. on their website). However, if the changes or additions are material or substantive, then in line with paragraphs 29 to 32 below, such changes should be actively brought to the attention of the data subject.

   依據GDPR前言第171點，對於在2018年5月25日之前已進行之運用行為，資料控管者應確保截至2018年5月25日時，該運用符合其透明化義務（以及GDPR下其他所有義務）。意即，在2018年5月25日之前，資料控管者應重新審查提供予當事人有關運用其個人資料（例如隱私聲明/通知等）的所有資訊，以確保其符合本指引所討論有關透明化之要求。若對此類資訊有所變更或增補，控管者應向當事人明確說明為遵循GDPR已實施該項變更。WP29建議應主動使當事人注意此變更或增補，控管者至少應公開揭露該資訊（例如公布於網站上）。然而，若為重大或實質性的變更或增補時，依據以下第29至32段，應主動使當事人注意此變更。

4. Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights[10]. The concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles. The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR. However, the quality, accessibility and comprehensibility of the information is as important as

[8] Article 5.2 of the GDPR obliges a data controller to demonstrate transparency (together with the five other principles relating to data processing set out in Article 5.1) under the principle of accountability.
GDPR第5條第2項要求資料控管者依據課責性原則證明透明化（連同第5條第1項規定與資料運用相關之其他五項原則）。

[9] The obligation upon data controllers to implement technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR is set out in Article 24.1.
GDPR第24條第1項規定資料控管者有義務採取技術性和組織性措施，確保並得以證明依GDPR執行運用。

the actual content of the transparency information, which must be provided to data subjects.
當資料控管者遵守透明化義務時，能使當事人得以判斷資料控管者和受託運用者是否可課責，並透過例如：提供或撤回「告知後同意」，和行使當事人權利來掌控其個人資料[10]。GDPR下之透明化概念是以使用者而非法律為中心，並透過許多條文中對資料控管者和受託運用者的特定具體要求而得以實現。GDPR第12至14條概述了該具體（資訊）要求。然而，資訊之品質、可得性和可理解性與應提供給當事人之透明資訊的實際內容同等重要。

5. The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. This is clear from Article 12 which provides that transparency applies at the following stages of the data processing cycle:
GDPR中的透明化要求於資料運用之法律依據與整個運用過程皆有適用。第12條明確規定，透明化適用於資料運用週期之以下階段：

- before or at the start of the data processing cycle, i.e. when the personal data is being collected either from the data subject or otherwise obtained;
在資料運用週期之前或開始時，即：自當事人蒐集或以其他方式取得個人資料時；
- throughout the whole processing period, i.e. when communicating with data subjects about their rights; and
在整個資料運用期間，即：與當事人就其權利進行溝通時; 以及
- at specific points while processing is ongoing, for example when data breaches occur or in the case of material changes to the processing.
在資料運用過程中的某些特定時點，例如在發生資料侵害或在運用行為有重大變更時。

The meaning of transparency
透明化之含義

6. Transparency is not defined in the GDPR. Recital 39 of the GDPR is informative as to the meaning and effect of the principle of transparency in the context of data processing:
GDPR並未定義何謂透明化。GDPR前言第39點就資料運用背景下透明化原則之含義和影響提供了相關資訊：

"*It should be transparent to natural persons that personal data concerning them are collected,*

[10] See, for example, the Opinion of Advocate General Cruz Villalon (9 July 2015) in the Bara case (Case C-201/14) at paragraph 74: *"the requirement to inform the data subjects about the processing of their personal data, which guarantees transparency of all processing, is all the more important since it affects the exercise by the data subjects of their right of access to the data being processed, referred to in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive".*
請參閱，例如巴拉案（案例C-201/14）中佐審官克魯茲·比利隆之意見（2015年7月9日），第74段：「*要求告知當事人關於其個人資料之運用以確保所有運用之透明化，這一點尤為重要，因影響當事人行使其依據95/46指令第12條對被運用資料之近用權，及第14條之拒絕權*」。

used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…"

「*個人資料之蒐集、使用、查詢或其他運用，應向該資料之自然人保持透明化，且應及於該個人資料所被運用或將被運用之程度。透明化原則要求關於個人資料運用之任何資訊或溝通方式應便於取得、易於理解且應使用清晰簡明之語言。透明化原則特別關注提供當事人控管者身分、運用資料之目的以及得以確保相關自然人資料運用之公正性和透明化的進一步資訊，並確保其有權利就受運用之個人資料進行確認和溝通。…*」

Elements of transparency under the GDPR

GDPR下透明化之要件

7. The key articles in relation to transparency in the GDPR, as they apply to the rights of the data subject, are found in Chapter III (Rights of the Data Subject). Article 12 sets out the general rules which apply to: the provision of information to data subjects (under Articles 13-14); communications with data subjects concerning the exercise of their rights (under Articles 15 - 22); and communications in relation to data breaches (Article 34). In particular Article 12 requires that the information or communication in question must comply with the following rules:

   由於GDPR下之透明化適用於當事人之權利，因此相關主要條款規範於第三章（當事人之權利）。第12條規定以下情形應適用之一般規則：向當事人提供資訊（第13-14條）；與當事人就其權利之行使進行溝通（第15-22條）；以及就資料侵害進行之溝通（第34條）。第12條特別要求相關資訊或溝通必須遵循下列規則：

   - it must be concise, transparent, intelligible and easily accessible (Article 12.1);
     必須簡潔、透明、易懂且便於取得（第12條第1項）；
   - clear and plain language must be used (Article 12.1)；
     必須使用清晰簡明之語言（第12條第1項）；
   - the requirement for clear and plain language is of particular importance when providing information to children (Article 12.1);
     清晰簡明語言之要求在向兒童提供資訊時尤為重要（第12條第1項）；
   - it must be in writing "*or by other means, including where appropriate, by electronic means*"

(Article 12.1);
必須以書面形式提供，「*或透過其他方式，包括在適當情況下，透過電子方式提供*」（第12條第1項）；

- where requested by the data subject it may be provided orally (Article 12.1) ; and
  若當事人提出要求，得以口頭提供資訊（第12條第1項）；以及
- it generally must be provided free of charge (Article 12.5).
  一般情形下必須無償提供資訊（第12條第5項）。

"Concise, transparent, intelligible and easily accessible"
「簡潔、透明、易懂且便於取得」

8. The requirement that the provision of information to, and communication with, data subjects is done in a "concise and transparent" manner means that data controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue. This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use. In an online context, the use of a layered privacy statement/ notice will enable a data subject to navigate to the particular section of the privacy statement/ notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues.
向當事人提供資訊和進行溝通之方式應「簡潔和透明」之要求，意味著資料控管者應該有效率地和簡潔地提供資訊/溝通，以避免資訊疲勞。此類資訊應和其他非隱私相關資訊（如契約條款或一般使用條款）做出明確之區分。在網路環境中，使用階層隱私聲明/通知將能夠引導當事人至其想要立即取得隱私聲明/通知之特定部分，而不需瀏覽大量文本以搜尋特定之項目。

9. The requirement that information is "intelligible" means that it should be understood by an average member of the intended audience. Intelligibility is closely linked to the requirement to use clear and plain language. An accountable data controller will have knowledge about the people they collect information about and it can use this knowledge to determine what that audience would likely understand. For example, a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children. If controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/ notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things.
資訊需「易於理解」之要求意味著該資訊應能夠被目標群眾的一般成員所理解。可理解

性與使用清晰簡明語言之要求密切相關。可歸責之資料控管者將會知悉其蒐集資料之當事人，並可使用這些資訊來確認群眾可能理解之內容。例如，蒐集專業工作人員個人資料之控管者可以假設其目標群眾比蒐集兒童個人資料之控管者具有更高之理解程度。若控管者不確定資訊的可理解性和透明化以及用戶介面/通知/政策等的有效性，控管者可透過某些機制加以測試，例如，透過用戶面板、可讀性測試、正式和非正式互動以及與產業團體、消費者權益保護團體和監管機關進行對話溝通，或酌情使用其他機制。

10. A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. This is also an important aspect of the principle of fairness under Article 5.1 of the GDPR and indeed is linked to Recital 39 which states that *"[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data..."* In particular, for complex, technical or unexpected data processing, WP29's position is that, as well as providing the prescribed information under Articles 13 and 14 (dealt with later in these guidelines), controllers should also separately spell out in unambiguous language what the most important *consequences* of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? In accordance with the principle of accountability and in line with Recital 39, data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data.

這些條款中概述之透明化原則的核心考量在於，當事人應能夠事先確認所需運用的資料範圍及後果為何，而不至於日後某一時點因其個人資料被使用之方式而感到意外。此亦為GDPR第5條第1項所規定公正原則下的一個重要面向，且與前言第39點相關，該前言指出「*應使自然人了解關於運用個人資料之風險、規則、安全維護措施和權利...*」。特別是對複雜的技術性或未預期之資料運用，WP29的立場與依據第13條和第14條提供前述資訊（本指引將於其後另做說明），控管者亦應使用明確的語言單獨說明該運用將產生的最重要*後果*：易言之，隱私聲明/通知中所描述之具體運用對當事人實際上會產生何種影響？依據課責性原則以及前言第39點，資料控管者應評估是否有涉及此類運用之自然人應注意之特殊風險。此方式有助於全面釐清可能對當事人在與保護其個人資料相關之基本權利和自由方面產生最大影響的資料運用類型。

11. The "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be

accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question (for example in an online layered privacy statement/ notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface, etc. These mechanisms are further considered below, including at paragraphs 33 to 40).

「便於取得」之要件意味著當事人無需搜尋；此類資訊於何處取得及如何取得，對當事人而言應立即且明顯，例如直接提供、透過連結、透過明確指示或以一般用語問答（例如，於網路分層的隱私聲明/通知中、於常見問題解答(FAQs)中、於當事人網路填寫表格時彈出視窗、或於互動式數位聊天機器人界面等。這些機制於以下第33至40段進一步考量）。

Example
示例

Every organisation that maintains a website should publish a privacy statement/ notice on the website. A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as “Privacy”, “Privacy Policy” or “Data Protection Notice”). Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.

每個經營網站的組織都應在其網站上公布隱私聲明/通知。隱私聲明/通知的直接連結應在該網站的每個頁面上以常用術語（例如「隱私」、「隱私政策」或「資料保護通知」）清楚表明。若因擺放位置或配色方式使內容或網址連結不明顯或難以在網頁上發現，則將認為其不便於取得。

For apps, the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than “two taps away” (e.g. by including a “Privacy”/ “Data Protection” option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public.

對於行動應用程式，相關必要資訊應在下載前從網路商店取得。應用程式安裝後，相關資訊仍需易於該程式取得。滿足此項要件方式之一係確保無須「點擊超過兩次」以取得資訊（例如透過在應用程式功能表中建立「隱私」/「資料保護」選項）。此外，該隱私資訊應針對特定應用程式，而非僅為擁有或向公眾提供該應用程式之公司的一般隱私政策。

WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected.

WP29建議，實務最佳做法是，於線上蒐集個人資料同時，應提供隱私聲明/通知之連結，或在蒐集個人資料的同一頁面上提供該資訊。

"Clear and plain language"

「清晰簡明之語言」

12. With *written* information (and where written information is delivered orally, or by audio/ audiovisual methods, including for vision-impaired data subjects), best practices for clear writing should be followed.[11] A similar language requirement (for "plain, intelligible language") has previously been used by the EU legislator[12] and is also explicitly referred to in the context of consent in Recital 42 of the GDPR[13]. The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear.

提供書面資訊（以及口頭傳遞書面資訊，或透過影音/視聽之方式，包括對視力受損之當事人），應遵循明確書寫之最佳實務做法[11]。歐盟立法者[12]曾使用過類似的語言要求（對於「簡明易懂之語言」），而GDPR前言第42點中，在有關同意之規範也明確提及了該項要求[13]。對清晰和簡明語言之要求意味著應盡可能以簡單的方式提供資訊，避免複雜的句子和語言結構。資訊應具體而明確；且不應以抽像或矛盾之措辭來表達，也不應留有做出不同解釋之空間。特別是運用個人資料之目的和法律依據必須是清楚的。

[11] See How to Write Clearly by the European Commission (2011), to be found at: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.
請參閱由歐盟執委會發行之如何明確書寫（2011），請查閱：https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.

[12] Article 5 of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts
1993年4月5日理事會第93/13 / EEC號指令第5條有關消費者契約中不公正之條款。

[13] Recital 42 states that a declaration of consent pre-formulated by a data controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.
前言第42點指出，資料控管者預先制定之同意聲明應以易於理解和易於取得之形式為之，且應使用清晰簡明之語言，且不應包含不公正之條款。

Poor Practice Examples

不良實務示例

The following phrases are not sufficiently clear as to the purposes of processing:

下列語句就於運用目的之解釋不夠明確：

- *"We may use your personal data to develop new services"* (as it is unclear what the "services" are or how the data will help develop them);

  「*我們可能會使用您的個人資料來開發新服務*」（該「服務」為何或該資料將如何協助開發皆不明確）；

- *"We may use your personal data for research purposes* (as it is unclear what kind of "research" this refers to); and

  「*我們可能會將您的個人資料用於研究目的*」（該「研究」為何並不明確）；及

- "We may use your personal data to offer personalised services" (as it is unclear what the "personalisation" entails).

  「*我們可能會使用您的個人資料以提供個人化服務*」（何謂「個人化」並不明確）。

Good Practice Examples[14]

優良實務示例[14]

- "*We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in* " (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);

  「*我們將保留您的購物歷史記錄並使用您之前購買產品的詳細資訊，以便為您提供我們認為您也會感興趣其他產品之建議*」（此語句清楚表示將運用何種類型之資料、當事人將成為精準廣告對象且其資料將用於達到此目的）；

[14] The requirement for transparency exists entirely independently of the requirement upon data controllers to ensure that there is an appropriate legal basis for the processing under Article 6.

對透明化之要求完全獨立於依據第6條資料控管者需確保資料運用有適當法律依據之要求。

- "*We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive*" (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and

  「*為了瞭解用戶如何使用我們的網站，以便我們可以改善網站的直觀性，我們將保留和評估您最近造訪我們網站之資訊以及就您於網站上點選不同區塊之行為進行分析。*」（此語句清楚表示將運用何種類型之資料以及控管者將進行何種類型之分析）；及

- "*We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read*" (it is clear what the personalisation entails and how the interests attributed to the data subject have been identified).

  「*我們將會記錄您所點擊之本網站文章，依據您所閱讀的文章等相關資訊辨識出您的興趣，並於本網站對您提供精準行銷*」（清楚表示個人化所需為何，以及如何辨識當事人之興趣）。

13. Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing. Paragraphs and sentences should be well structured, utilising bullets and indents to signal hierarchical relationships. Writing should be in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax makes sense in the second language(s) so that the translated text does not have to be deciphered or re-interpreted. (A translation in one or more other languages should be provided where the controller targets[15] data subjects speaking those languages.)

    另應避免使用諸如「可能」、「也許」、「某些」、「經常」和「或許」之語言後置修飾語。若資料控管者選擇使用此種不確定語言，依據課責性原則，控管者應要能夠證明

無法避免使用該語言之原因以及如何不損害運用之公正性。段落和句子之結構應該合理，並利用項目符號和縮排來顯示階層關係。應以主動式而非被動式書寫，且應該避免使用過多的名詞。提供給當事人之資訊不應包含過多法律、技術或專業語言或術語。當資訊被翻譯成一種或多種語言時，資料控管者應確保所有翻譯皆為準確的，且用語和語法在第二種語言中是合理的，使翻譯之內容不需被闡釋或重新解釋。（當控管者針對[15]的當事人使用某些語言時，控管者應提供一種或多種其他語言之翻譯。）

Providing information to children and other vulnerable people

向兒童和其他弱勢群體提供資訊

14. Where a data controller is targeting children[16] or is, or should be, aware that their goods/ services are particularly utilised by children (including where the controller is relying on the consent of the child)[17], it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/ information is being directed at them.[18] A useful example of child-centred language used as an alternative to the original legal language can be found in the "UN Convention on the Rights of the Child in Child Friendly Language".[19]

當資料控管者以兒童[16]為對象，或是（或必須）知悉兒童使用其商品/服務之情形（包括控管者需獲得兒童之同意時）[17]，控管者應確保所使用語言之詞彙、語氣和風格需適合兒童並可與其產生共鳴，以使接收該資訊之兒童可意識到該訊息/資訊是直接對其所為。[18]「聯合國兒童友好語言之兒童權利公約」提供了一種以兒童為中心的語言以替代原始法律語言之範例。[19]

---

[15] For example, where the controller operates a website in the language in question and/or offers specific country options and/or facilitates the payment for goods or services in the currency of a particular member state then these may be indicative of a data controller targeting data subjects of a particular member state.
例如，當控管者以系爭之語言經營網站和/或提供特定國家選項和/或提供以特定成員國之貨幣支付商品或服務之情形下，這些皆可作為資料控管者針對特定成員國當事人之指標。

[16] The term "child" is not defined under the GDPR, however WP29 recognises that, in accordance with the UN Convention on the Rights of the Child, which all EU Member States have ratified, a child is a person under the age of 18 years.
GDPR並未定義「兒童」一詞，但WP29認為，依據所有歐盟成員國簽署之「聯合國兒童權利公約」，兒童係指未滿18歲之人。

[17] i.e. children of 16 years or older (or, where in accordance with Article 8.1 of the GDPR Member State national law has set the age of consent at a specific age between 13 and 16 years for children to consent to an offer for the provision of information society services, children who meet that national age of consent).
即16歲或16歲以上之兒童（或依據GDPR第8條第1項，成員國國家法律就兒童對於資訊社會服務之同意設立介於13歲至16歲間的特定年齡門檻，而該兒童達到該國家法定同意年齡）。

[18] Recital 38 states that "Children merit special protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data". Recital 58 states that "Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand".
前言第38點指出「有鑑於兒童可能未盡知悉其個人資料運用之風險、後果及相關安全維護措施與其權利，兒童就其個人資料應受到特別保護」。前言第58點指出「有鑑於兒童應受到特別保護，任何提供予兒童之資訊及溝通應採用兒童易於理解之清晰簡明之語言」。

[19] https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf

15. WP29's position is that transparency is a free-standing right which applies as much to children as it does to adults. WP29 emphasises in particular that children do not lose their rights as data subjects to transparency simply because consent has been given/ authorised by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies. While such consent will, in many cases, be given or authorised on a once-off basis by the holder of parental responsibility, a child (like any other data subject) has an ongoing right to transparency throughout the continuum of their engagement with a data controller. This is consistent with Article 13 of the UN Convention on the Rights of the Child which states that a child has a right to freedom of expression which includes the right to seek, receive and impart information and ideas of all kinds.[20] It is important to point out that, while providing for consent to be given on behalf of a child when under a particular age,[21] Article 8 *does not provide* for transparency measures to be directed at the holder of parental responsibility who gives such consent. Therefore, data controllers have an obligation in accordance with the specific mentions of transparency measures addressed to children in Article 12.1 (supported by Recitals 38 and 58) to ensure that where they target children or are aware that their goods or services are particularly utilised by children of a literate age, that any information and communication should be conveyed in clear and plain language or in a medium that children can easily understand. For the avoidance of doubt however, WP29 recognises that with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency.

WP29之立場為，透明化是一種獨立的權利，同等適用於兒童及成年人。WP29特別強調，兒童不會因在GDPR第8條適用之情況下，由於法定代理人所給予或授權同意，而失去身為資料當事人所擁有之透明化權利。雖然在許多情況下，此種同意將由法定代理人一次性給予或授權，但兒童（如同其他當事人）在與控管者互動的整個過程中，始終享有透明化之權利。這符合「聯合國兒童權利公約」第13條，該條規定兒童有言論自由之權利，包括尋求、接受和傳播各類資訊和思想之權利。[20]必須指出，雖然第8條並未針對一定年齡下兒童自己所為之同意[21]，就給予此類同意權之法定代理人訂定透明化措施。因此，依據第12條第1項中針對兒童透明化措施之特定要求（前言第38點和第58點亦支持），當資

[20] Article 13 of the UN Convention on the Rights of the Child states that: "The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice."
聯合國兒童權利公約第13條規定：「兒童應享有言論自由之權利；此權利包括尋求、接受和傳播各類資訊和思想之自由，不分國界，無論是以言詞、書面或印刷、藝術形式，或透過兒童選擇之其他媒介。」

[21] See footnote 17 above.
請參閱前註17。

料控管者是針對兒童，或知悉其商品或服務是由識字年齡兒童使用時，其有義務確認任何資訊和溝通都應以清晰簡明的語言或兒童可輕易理解之媒介傳達。然而，為避免爭議，WP29認為，對於年紀很小或尚不識字的兒童，亦可向法定代理人提供透明化措施，因在大多數情況下，即使是最基本之書面或非書面關於透明化的訊息，這些兒童也不太可能理解。

16. Equally, if a data controller is aware that their goods/ services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects.[22] This relates to the need for a data controller to assess its audience's likely level of understanding, as discussed above at paragraph 9.

同樣，若資料控管者知悉其商品/服務是由（或針對）社會其他弱勢成員（包括身心障礙人士或可能難以獲得資訊之人）所使用，在評估如何確保其符合與當事人相關之透明化義務時，控管者應考量此類型當事人之易受傷害性。[22]如前文第9段所述，此與資料控管者評估其目標受眾可能之理解程度相關。

"In writing or by other means"

「以書面或其他方式」

17. Under Article 12.1, the default position for the provision of information to, or communications with, data subjects is that the information is in writing.[23] (Article 12.7 also provides for information to be provided in combination with standardised icons and this issue is considered in the section on visualisation tools at paragraphs 49 to 53). However, the GDPR also allows for other, unspecified "means" including electronic means to be used. WP29's position with regard to written electronic means is that where a data controller maintains (or operates, in part or in full, through) a website, WP29 recommends the use of layered privacy statements/ notices, which allow website visitors to navigate to particular aspects of the relevant privacy statement/ notice that are of most interest to them (see more on layered privacy statements/ notices at paragraph 35 to 37).[24] However, the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (whether in a digital or paper format) which can be easily accessed by a data subject should they wish to consult the entirety of the information addressed to them. Importantly, the use of a layered approach is not confined only to written electronic means for providing information

[22] For example, the UN Convention on the Rights of Persons with Disabilities requires that appropriate forms of assistance and support are provided to persons with disabilities to ensure their access to information.
例如，「聯合國身心障礙者權利公約」要求向身心障礙者提供適當形式之援助和支持，以確保其獲得資訊。

to data subjects. As discussed at paragraphs 35 to 36 and 38 below, a layered approach to the provision of information to data subjects may also be utilised by employing a combination of *methods* to ensure transparency in relation to processing.

依據第12條第1項，向當事人提供資訊或溝通之基本方式係以書面為之。[23]（第12條第7項亦規定了與標準化圖示一併提供之資訊，此議題將於第49至53段關於視覺化工具部分另加說明）。然而，GDPR亦允許使用其他未指明之「方式」，包括使用電子方式。WP29對書面電子方式之立場為，當在資料控管者經營（或其營運係部分或全部透過）網站之情況下，WP29建議使用分層隱私聲明/通知，允許網站使用者可瀏覽其最感興趣的相關隱私聲明/通知（有關分層隱私聲明/通知的進一步資訊請參閱第35至37段）。[24]然而，提供予當事人之全部資訊應放置於同一個位置或以一份完整之文件呈現（無論係數位或紙本格式），使當事人欲查看整份文件時，即可以輕鬆地取得所提供之資訊。重要的是，分層方式的使用不僅限於以書面電子方式向當事人提供資訊時。如以下第35至36段和第38段所述，選擇使用各種方式之組合來確保關於運用的透明化時，亦可遵循分層方式向當事人提供資訊。

18. Of course, the use of digital layered privacy statements/ notices is not the only written electronic means that can be deployed by controllers. Other electronic means include "just-in-time" contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards. Non-written electronic means which may be used *in addition* to a layered privacy statement/ notice might include videos and smartphone or IoT voice alerts.[25] "Other means", which are not necessarily electronic, might include, for example, cartoons, infographics or flowcharts. Where transparency information is directed at children specifically, controllers should consider what types of measures may be particularly accessible to children (e.g. these might be comics/ cartoons, pictograms, animations, etc. amongst other measures).

當然，數位分層隱私聲明/通知並非控管者可使用的唯一書面電子方式。其他電子方式包括「即時」上下文彈出通知、3D觸碰或滑鼠游標懸停通知（hover-over notices）以及隱私儀表板（privacy dashboards）。除了分層隱私聲明/通知*以外*，可使用之非書面電子方式亦可包括影音和智能手機或物聯網（IoT）語音警示。[25]「其他方式」並非一定為電子方式，亦可包括如卡通、資訊圖表或流程圖。當透明化資訊是專門針對兒童之情況下，控

[23] Article 12.1 refers to "language" and states that the information shall be provided in writing, or by other means, including, where appropriate, by electronic means.
第12條第1項提及「語言」，並指出資訊應以書面或其他方式提供，包括在適當情況下以電子方式提供。
[24] The WP29's recognition of the benefits of layered notices has already been noted in Opinion 10/2004 on More Harmonised Information Provisions and Opinion 02/2013 on apps on smart devices.
WP29對階層通知益處之認可已展現於第10/2004號關於更協調之資訊條款意見及第02/2013號關於智能設備上之行動應用程式意見。
[25] These examples of electronic means are indicative only and data controllers may develop new innovative methods to comply with Article 12.
這些電子方式之示例僅供參考，資料控管者可發展創新方式以符合第12條之規範。

管者應考量何種類型之措施特別適合兒童使用（例如可能包括漫畫/卡通、圖像以及動畫等其他措施）。

19. It is critical that the method(s) chosen to provide the information is/are appropriate to the particular circumstances, i.e. the manner in which the data controller and data subject interact or the manner in which the data subject's information is collected. For example, only providing the information in electronic written format, such as in an online privacy statement/ notice may not be appropriate/ workable where a device that captures personal data does not have a screen (e.g. IoT devices/ smart devices) to access the website/ display such written information. In such cases, appropriate alternative *additional* means should be considered, for example providing the privacy statement/ notice in hard copy instruction manuals or providing the URL website address (i.e. the specific page on the website) at which the online privacy statement/ notice can be found in the hard copy instructions or in the packaging. Audio (oral) delivery of the information could also be additionally provided if the screenless device has audio capabilities. WP29 has previously made recommendations around transparency and provision of information to data subjects in its Opinion on Recent Developments in the Internet of Things[26] (such as the use of QR codes printed on internet of things objects, so that when scanned, the QR code will display the required transparency information). These recommendations remain applicable under the GDPR.

重要的是，選擇提供資訊之方式需符合特定情況，即資料控管者和當事人互動之方式或蒐集當事人資訊之方式。例如，若蒐集個人資料之設備並無螢幕（例如物聯網設備/智能設備）以供造訪網站/顯示書面資訊，則僅提供電子書面格式之資訊（例如網路隱私聲明/通知）可能不適合/不可行。在此情況下，應考量*其他*適當之替代方式，例如在紙本說明手冊中提供隱私聲明/通知，或在紙本說明書或外包裝提供網路隱私聲明/通知的URL網址（即網站上之特定頁面）。若該無螢幕之設備具有語音功能，則亦可另以語音（口頭）提供相關資訊。WP29先前在其關於物聯網近期發展意見書中[26]曾就透明化和提供當事人資訊提出建議（例如使用刊印在物聯網物件上之QR碼，當掃描該QR碼時，將顯示所需之透明化資訊）。此建議於GDPR仍有適用。

"..the information may be provided orally"

「..得以口頭提供資訊」

20. Article 12.1 specifically contemplates that information may be provided orally to a data subject on request, provided that their identity is proven by other means. In other words, the means employed should be more than reliance on a mere assertion by the individual that they are

[26] WP29 Opinion 8/2014 adopted on 16 September 2014
WP29第8/2014號意見於2014年9月16日通過。

a specific named person and the means should enable the controller to verify a data subject's identity with sufficient assurance. The requirement to verify the identity of the data subject before providing information orally only applies to information relating to the exercise by a specific data subject of their rights under Articles 15 to 22 and 34. This precondition to the provision of oral information cannot apply to the provision of general privacy information as outlined in Articles 13 and 14, since information required under Articles 13 and 14 must also be made accessible to *future* users/ customers (whose identity a data controller would not be in a position to verify). Hence, information to be provided under Articles 13 and 14 may be provided by oral means without the controller requiring a data subject's identity to be proven.

第12條第1項特別考量若當事人之身分可透過其他方式確認，得應當事人之要求向其口頭提供資訊。易言之，所採行之方式不得僅基於當事人聲稱其為該特定人士，且該方式應使控管者得充分核實當事人之身分。在口頭提供資訊前需核實當事人身分之要求僅適用於當該資訊與特定當事人依據第15條至第22條和第34條行使其權利有所關聯時。提供口頭資訊之先決條件不適用於第13條和第14條所規範一般隱私資訊之提供，因第13條和第14條所要求之資訊亦需提供予未來的用戶/客戶（資料控管者無法核實其身分）。因此，依第13條和第14條規定所應提供之資訊，得未經控管者核實當事人之身分，以口頭方式提供。

21. The oral provision of information required under Articles 13 and 14 does not necessarily mean oral information provided on a person-to-person basis (i.e. in person or by telephone). Automated oral information may be provided in addition to written means. For example, this may apply in the context of persons who are visually impaired when interacting with information society service providers, or in the context of screenless smart devices, as referred to above at paragraph 19. Where a data controller has chosen to provide information to a data subject orally, or a data subject requests the provision of oral information or communications, WP29's position is that the data controller should allow the data subject to re-listen to pre-recorded messages. This is imperative where the request for oral information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information in written format. The data controller should also ensure that it has a record of, and can demonstrate (for the purposes of complying with the accountability requirement): (i) the request for the information by oral means, (ii) the method by which the data subject's identity was verified (where applicable – see above at paragraph 20) and (iii) the fact that information was provided to the data subject.

第13條和第14條所規範之口頭提供資訊並非必須以人對人之方式為之（即親自或透過電話）。除書面方式外，亦可提供自動口頭資訊。例如，當視力受損之人與資訊社會服務提供者互動時或如前文第19段所述智能設備並無螢幕時，即可適用此種方式。若資料控

管者選擇以口頭提供資訊予當事人，或當事人要求提供口頭資訊或溝通，WP29之立場為資料控管者應允許當事人可重複聽取預先錄製之資訊。當口頭資訊之要求涉及有視覺障礙之當事人或涉及可能難以書面形式獲得或理解資訊之其他當事人時，此要件係為必要的。資料控管者另應確保其擁有下列紀錄並可提出證明（以符合課責性之要求）：（i）以口頭方式提出資訊之要求，（ii）核實當事人身分之方式（如適用 – 請參閱前文第20段）以及（iii）向當事人提供資訊之事實。

"Free of charge"

「無償」

22. Under Article 12.5,[27] data controllers cannot generally charge data subjects for the provision of information under Articles 13 and 14, or for communications and actions taken under Articles 15 - 22 (on the rights of data subjects) and Article 34 (communication of personal data breaches to data subjects).[28] This aspect of transparency also means that any information provided under the transparency requirements cannot be made conditional upon financial transactions, for example the payment for, or purchase of, services or goods.[29]

第12條第5項規定[27]，資料控管者一般不得對依據第13條和第14條所應提供予當事人之資訊，或依據第15-22條（關於當事人的權利）及第34條（就個人資料侵害與當事人進行溝通）採取之溝通和行動收取費用。[28]透明化之此點要素也表示依據透明化要求提供之任何資訊皆不得以交易為條件，例如支付或購買服務或貨物。[29]

Information to be provided to the data subject – Articles 13 & 14

應提供予當事人之資訊 - 第13條和第14條

---

[27] This states that "Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge."
該條款規定「依據第13條和第14條提供之資訊以及依據第15條至第22條和第34條所採取之任何溝通和任何行動均應無償提供。」

[28] However, under Article 12.5 the controller may charge a reasonable fee where, for example, a request by a data subject in relation to the information under Article 13 and 14 or the rights under Articles 15 - 22 or Article 34 is excessive or manifestly unfounded. (Separately, in relation to the right of access under Article 15.3 a controller may charge a reasonable fee based on administrative costs for any further copy of the personal data which is requested by a data subject).
然而，依據第12條第5項，例如當事人就第13條和第14條規定之資訊或第15條至第22條或第34條規定之權利所提出之請求過度或明顯無依據時，控管者可收取合理之費用。（此外，關於第15條第3項近用之權利，若當事人要求任何進一步的個人資料副本，控管者得基於行政成本收取合理費用）。

[29] By way of illustration, if a data subject's personal data is being collected in connection with a purchase, the information which is required to be provided under Article 13 should be provided prior to payment being made and at the point at which the information is being collected, rather than after the transaction has been concluded. Equally though, where free services are being provided to the data subject, the Article 13 information must be provided prior to, rather than after, sign-up given that Article 13.1 requires the provision of the information "at the time when the personal data are obtained".
舉例來說，若有關當事人個人資料之蒐集與購買行為相關，依據第13條要求提供之資訊則應在付款前以及蒐集資料時提供，而非在交易結束後。同樣，在向當事人提供免費服務之情況下，第13條之資訊必須在註冊前而非註冊後提供，因第13條第1項要求資訊之提供需「在取得個人資料時」。

Content

內容

23. The GDPR lists the categories of information that must be provided to a data subject in relation to the processing of their personal data where it is collected from the data subject (Article 13) or obtained from another source (Article 14). The **table in the Annex** to these guidelines summarises the categories of information that must be provided under Articles 13 and 14. It also considers the nature, scope and content of these requirements. For clarity, WP29's position is that there is no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively. All of the information across these sub-articles is of equal importance and must be provided to the data subject.
GDPR列舉出有關當運用當事人之個人資料係從當事人取得（第13條）或從其他來源蒐集（第14條）時，必須提供予當事人之資訊類型。本指引**附錄表格**綜整了依據第13條和第14條必須提供之資訊類型，亦將這些要求之性質、範圍和內容納入考量。為臻明確，WP29之立場為，第13條和第14條的第1項及第2項下所應提供之資訊情狀並無區別。這些項次中的所有資訊皆具有同等重要性，且必須提供予當事人。

"Appropriate measures"

「適當之措施」

24. As well as content, the form and manner in which the information required under Articles 13 and 14 should be provided to the data subject is also important. The notice containing such information is frequently referred to as a data protection notice, privacy notice, privacy policy, privacy statement or fair processing notice. The GDPR does not prescribe the format or modality by which such information should be provided to the data subject but does make it clear that it is the data controller's responsibility to take "appropriate measures" in relation to the provision of the required information for transparency purposes. This means that the data controller should take into account all of the circumstances of the data collection and processing when deciding upon the appropriate modality and format of the information provision. In particular, appropriate measures will need to be assessed in light of the product/ service user experience. This means taking account of the device used (if applicable), the nature of the user interfaces/ interactions with the data controller (the user "journey") and the limitations that those factors entail. As noted above at paragraph 17, WP29 recommends that where a data controller has an online presence, an online layered privacy statement/ notice should be provided.
除內容外，依第13條和第14條要求應提供予當事人之資訊的格式和方式亦同等重要。包含此類資訊之通知一般被稱作資料保護通知、隱私通知、隱私政策、隱私聲明或公正運

用通知。GDPR並未規定應向當事人提供此類資訊之格式或形式，但明確規範資料控管者有責任依透明化目的就所需提供之資訊採取「適當措施」。此意味著資料控管者在決定提供資訊之適當格式或形式時，應考量資料蒐集和運用的所有情狀。尤其是，必須依據產品/服務用戶體驗以評估適當之措施。此意味著應考量所使用之設備（如適用）、用戶界面/與控管者互動之性質（用戶「旅程」）以及這些情況所產生之限制。如前文第17段所述，WP29建議，若資料控管者擁有網路平台，則應提供網路分層隱私聲明/通知。

25. In order to help identify the most appropriate modality for providing the information, in advance of "going live", data controllers may wish to trial different modalities by way of user testing (e.g. hall tests, or other standardised tests of readability or accessibility) to seek feedback on how accessible, understandable and easy to use the proposed measure is for users. (See also further comments above on other mechanisms for carrying out user testing at paragraph 9). Documenting this approach should also assist data controllers with their accountability obligations by demonstrating how the tool/ approach chosen to convey the information is the most appropriate in the circumstances.

為了協助確認提供資訊最合適之方式，在「上線」之前，資料控管者可能希望透過用戶測試（例如，廳堂測試（hall tests）或其他可閱讀性或可造訪性之標準化測試），嘗試不同模式，以尋求有關用戶可造訪性、易理解性和易使用性建議措施之回饋意見。（請另參閱前文第9段關於進行用戶測試之其他機制的進一步評論）。記錄此類嘗試可使資料控管者展示在特定情況下已選擇最適當傳達資訊之工具/方式，以協助資料控管者履行其課責性之義務。

Timing for provision of information

提供資訊之時點

26. Articles 13 and 14 set out information which must be provided to the data subject at the commencement phase of the processing cycle[30]. Article 13 applies to the scenario where the data is collected from the data subject. This includes personal data that:

第13條和第14條規定必須在資料運用週期的開始階段向當事人提供資訊[30]。第13條適用於從當事人蒐集資料之情況。包含當個人資料：

- a data subject consciously provides to a data controller (e.g. when completing an online form);

[30] Pursuant to the principles of fairness and purpose limitation, the organisation which collects the personal data from the data subject should always specify the purposes of the processing at the time of collection. If the purpose includes the creation of inferred personal data, the intended purpose of creating and further processing such inferred personal data, as well as the categories of the inferred data processed, must always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose in compliance with Article 13.3 or Article 14.4.
依據公正和目的限縮原則，從當事人蒐集個人資料之組織應在蒐集時即具體說明運用之目的。若其目的包括建立推定性個人資料（inferred data）、企圖建立並進一步運用此類推定性個人資料以及將運用的推定資料之類別，控管者必須在蒐集時或依據第13條第3項或第14條第4項基於新目的而欲進階運用個人資料前，就其目的與當事人進行溝通。

or

係當事人有意識地提供給資料控管者（例如，當完成網路表格時）；或

- a data controller collects from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors).
  係資料控管者透過觀察從當事人蒐集（例如，使用自動資料獲取設備或資料獲取軟體，例如相機、網路設備、Wi-Fi跟踪、無線射頻辨識（RFID）或其他類型之感應器）。

Article 14 applies in the scenario where the data have not been obtained from the data subject. This includes personal data which a data controller has obtained from sources such as:
第14條適用於非從當事人取得資料之情況。此包括資料控管者由以下來源取得個人資料：

- third party data controllers; 第三方資料控管者；
- publicly available sources; 公眾來源；
- data brokers; or 資料仲介；或
- other data subjects. 其他當事人。

27. As regards timing of the provision of this information, providing it in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 applies, under Article 13.1 the information must be provided *"at the time when personal data are obtained"*. In the case of indirectly obtained personal data under Article 14, the timeframes within which the required information must be provided to the data subject are set out in Article 14.3 (a) to (c) as follows:
有關提供資訊的時間，及時提供這些資訊是透明化義務和公正運用資料義務的關鍵要素。在適用第13條之情況下，依據第13條第1項，必須「*在取得個人資料時*」提供資訊。在依據第14條間接取得個人資料之情況下，必須向當事人提供所需資訊的時間範圍，依第14條第3項第a至c款規定如下：

- The general requirement is that the information must be provided within a "reasonable period" after obtaining the personal data and no later than one month, *"having regard to the specific circumstances in which the personal data are processed"* (Article 14.3(a)).
  一般要求為，必須在取得個人資料後的「合理期限」內提供資訊，且不得遲於一個月，「*考量到運用個人資料之具體情狀*」（第14條第3項第a款）。

- The general one-month time limit in Article 14.3(a) may be further curtailed under Article 14.3(b),[31] which provides for a situation where the data are being used for communication with the data subject. In such a case, the information must be provided at the latest at the time of the first communication with the data subject. If the first communication occurs prior to the

one-month time limit after obtaining the personal data, then the information must be provided *at the latest* at the time of the first communication with the data subject notwithstanding that one month from the point of obtaining the data has not expired. If the first communication with a data subject occurs more than one month after obtaining the personal data then Article 14.3(a) continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

第14條第3項第a款規定之一個月期限，於資料係用於與當事人溝通之情況下，依據第14條第3項第b款得加以縮減[31]。於此情形下，最遲須在與當事人進行第一次溝通時提供資訊。若第一次溝通發生在取得個人資料後的一個月期限內，則*最遲*必須在第一次與當事人溝通時提供資訊，即使從取得資料開始的一個月期限尚未到期。若第一次溝通發生在取得個人資料後之一個月後，則仍應適用第14條第3項第a款，因此第14條之資訊最遲須在取得資料的一個月內提供予當事人。

- The general one-month time limit in Article 14.3(a) can also be curtailed under Article 14.3(c)[32] which provides for a situation where the data are being disclosed to another recipient (whether a third party or not)[33]. In such a case, the information must be provided at the latest at the time of the first disclosure. In this scenario, if the disclosure occurs prior to the one-month time limit, then the information must be provided *at the latest* at the time of that first disclosure, notwithstanding that one month from the point of obtaining the data has not expired. Similar to the position with Article 14.3(b), if any disclosure of the personal data occurs more than one month after obtaining the personal data, then Article 14.3(a) again continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

  第14條第3項第a款規定之一個月期限，於資料向另一接收者(無論是否為第三方)[32]揭露時，依據第14條第3項第c款規定得加以縮減[33]。於此情形下，必須最遲在第一次揭露時提供資訊。若揭露發生於一個月期限之前，則*最遲*必須在第一次揭露時提供資訊，即使從取得資料開始的一個月期限尚未屆至。與第14條第3項第b款之立場相似，若在取得個

[31] The use of the words *"if the personal data are to be used for.."* in Article 14.3(b) indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.
在第14條第3項第b款中使用「*若個人資料用於...*」一詞，表示對第14條第3項第a款規定最長期限一般立場之特定情況說明，而非替代之。

[32] The use of the words *"if a disclosure to anther recipient is envisaged..."* in Article 14.3(c) likewise indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.
在第14條第3項第c款中使用「*若預計向他人揭露個人資料...*」一詞，同樣表示對第14條第3項第a款規定最長期限一般立場之特定情況說明，而非替代之。

[33] Article 4.9 defines "recipient" and clarifies that a recipient to whom personal data are disclosed does not have to be a third party. Therefore, a recipient may be a data controller, joint controller or processor.
第4條第9款定義何謂「接收者」，並闡明揭露個人資料之接收者不一定為第三方。因此，接收者亦可為資料控管者、共同控管者或受託運用者。

人資料一個月後始發生個人資料之揭露，則第14條第3項第a款仍繼續適用，因此第14條之資訊最遲須在取得資料的一個月內提供予當事人。

28. Therefore, in any case, the maximum time limit within which Article 14 information must be provided to a data subject is one month. However, the principles of fairness and accountability under the GDPR require data controllers to always consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that processing, when deciding at what point to provide the Article 14 information. Accountability requires controllers to demonstrate the rationale for their decision and justify why the information was provided at the time it was. In practice, it may be difficult to meet these requirements when providing information at the 'last moment'. In this regard, Recital 39 stipulates, amongst other things, that data subjects should be *"made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing"*. Recital 60 also refers to the requirement that the data subject be informed of the existence of the processing operation and its purposes in the context of the principles of fair and transparent processing. For all of these reasons, WP29's position is that, wherever possible, data controllers should, in accordance with the principle of fairness, provide the information to data subjects well in advance of the stipulated time limits. Further comments on the appropriateness of the timeframe between notifying data subjects of the processing operations and such processing operations actually taking effect are set out in paragraphs 30 to 31 and 48.

因此，在任何情況下，必須向當事人提供第14條資訊之最長期限為一個月。然而，在決定提供第14條資訊之時點時，GDPR之公正和課責原則要求資料控管者隨時考量當事人之合理期待、該項運用對當事人之影響以及當事人就該運用得以行使之權利。課責性要求控管者證明其決定之理由及於某時點提供資訊之正當性。實際上，於「最後時點」提供資訊可能難以符合上述要求。有鑑於此，前言第39點敘明，除其他事項外，應使當事人「*知悉與運用個人資料相關之風險、規則、安全維護措施和權利，以及如何行使和此類運用相關之權利*」。前言第60點亦提及在公正和透明化運用原則背景下，應向當事人通知運用作業的存在及其目的。基於以上原因，WP29之立場為，在可能的情況下，依據公正原則資料控管者應提前於規定期限內妥為向當事人提供資訊。關於就運用作業通知當事人與實際發生此類運用作業之間的適當時間點，在第30至31段和第48段中有進一步說明。

Changes to Article 13 and Article 14 information

第13條和第14條資訊之變更

29. Being accountable as regards transparency applies not only at the point of collection of

personal data but throughout the processing life cycle, irrespective of the information or communication being conveyed. This is the case, for example, when changing the contents of existing privacy statements/ notices. The controller should adhere to the same principles when communicating both the initial privacy statement/ notice and any subsequent substantive or material changes to this statement/ notice. Factors which controllers should consider in assessing what is a substantive or material change include the impact on data subjects (including their ability to exercise their rights), and how unexpected/ surprising the change would be to data subjects. Changes to a privacy statement/ notice that should always be communicated to data subjects include inter alia: a change in processing purpose; a change to the identity of the controller; or a change as to how data subjects can exercise their rights in relation to the processing. Conversely, an example of changes to a privacy statement/ notice which are not considered by WP29 to be substantive or material include corrections of misspellings, or stylistic/ grammatical flaws. Since most existing customers or users will only glance over communications of changes to privacy statements/ notices, the controller should take all measures necessary to ensure that these changes are communicated in such a way that ensures that most recipients will actually notice them. This means, for example, that a notification of changes should always be communicated by way of an appropriate modality (e.g. email, hard copy letter, pop-up on a webpage or other modality which will effectively bring the changes to the attention of the data subject) specifically devoted to those changes (e.g. not together with direct marketing content), with such a communication meeting the Article 12 requirements of being concise, transparent, intelligible, easily accessible and using clear and plain language. References in the privacy statement/notice to the effect that the data subject should regularly check the privacy statement/notice for changes or updates are considered not only insufficient but also unfair in the context of Article 5.1(A). Further guidance in relation to the timing for notification of changes to data subjects is considered below at paragraph 30 to 31.

對透明化之課責性不僅適用於蒐集個人資料時，且適用於整個資料運用過程，無論傳達之資訊或溝通為何。例如，更改現有隱私聲明/通知內容之情形。在溝通最初的隱私聲明/通知及對該聲明/通知為任何後續實質或重大變更時，控管者皆應遵循相同之原則。控管者在評估何謂實質或重大變更時，應考量之因素包含：對當事人之影響（包括其行使權利之能力），以及當事人對該變更感到意外/訝異之程度。必須與當事人進行溝通的隱私聲明/通知變更包括：運用目的之變更；控管者身分之變更；或當事人行使與資料運用相關權利之變更。反之，某些變更並非WP29所認為之實質或重大的隱私聲明/通知變更，例如包括錯誤拼寫或文體/文法瑕疵之更正。由於大多現有客戶或用戶僅會快速瀏覽隱私聲明/通知變更之通知，因此控管者應採取一切必要措施，以確保傳達之方式可使大多數

收件人實際注意到該變更。此意味著，例如，以適當的方式（例如：電子郵件、書面信件、彈出頁面或其他能有效引起當事人注意之方式），專門針對該變更進行通知(例如：該通知與行銷內容分開)，且傳達方式需符合第12條要求之簡潔、透明、易懂、易於取得和使用清晰簡明之語言。僅於隱私聲明/通知中提及當事人應定期檢查隱私聲明/通知之變更或更新，不僅將被視為不充足，亦不符合第5條第1項第a款中之公正性。有關通知當事人變更之時點的其他指導請參閱以下第30至31段。

Timing of notification of changes to Article 13 and Article 14 information
通知第13條和第14條資訊變更之時點

30. The GDPR is silent on the timing requirements (and indeed the methods) that apply for notifications of changes to information that has previously been provided to a data subject under Article 13 or 14 (excluding an intended further purpose for processing, in which case information on that further purpose must be notified prior to the commencement of that further processing as per Articles 13.3 and 14.4 – see below at paragraph 45). However, as noted above in the context of the timing for the provision of Article 14 information, the data controller must again have regard to the fairness and accountability principles in terms of any reasonable expectations of the data subject, or the potential impact of those changes upon the data subject. If the change to the information is indicative of a fundamental change to the nature of the processing (e.g. enlargement of the categories of recipients or introduction of transfers to a third country) or a change which may not be fundamental in terms of the processing operation but which may be relevant to and impact upon the data subject, then that information should be provided to the data subject well in advance of the change actually taking effect and the method used to bring the changes to the data subject's attention should be explicit and effective. This is to ensure the data subject does not "miss" the change and to allow the data subject a reasonable timeframe for them to (a) consider the nature and impact of the change and (b) exercise their rights under the GDPR in relation to the change (e.g. to withdraw consent or to object to the processing).
GDPR對於原依第13條或第14條(除意圖為其他目的之運用外。該情形下，依第13條第3項及第14條第4項，應於開始運用前即為通知—請參閱以下第45段)提供予當事人之資訊變更時，通知當事人該項變更之時點要求（及方式）並無規定。然而，如前文關於第14條資訊提供時點中所述，資料控管者必須再次考量在公正性和課責性原則下，當事人的任何合理期待或該項變更對當事人造成之潛在影響。若資訊之變更顯示運用的本質發生根本的變化（例如擴大接收者之類別或將傳輸至第三國）或雖變更對運用作業並無根本性之影響，但也許與當事人相關並對其產生影響，則這些資訊應在變更實際生效前完整地提供予當事人，且用於使當事人注意到該變更之方式必須係清楚且有效的。如此是為了確保當事人不至「錯過」變更，且使其在合理的時間範圍內得（a）考量該變更之本質

和影響，以及（b）行使其在GDPR下關於該變更之權利（例如撤回同意或拒絕運用）。

31. Data controllers should carefully consider the circumstances and context of each situation where an update to transparency information is required, including the potential impact of the changes upon the data subject and the modality used to communicate the changes, and be able to demonstrate how the timeframe between notification of the changes and the change taking effect satisfies the principle of fairness to the data subject. Further, WP29's position is that, consistent with the principle of fairness, when notifying such changes to data subjects, a data controller should also explain what will be the likely impact of those changes on data subjects. However, compliance with transparency requirements does not "whitewash" a situation where the changes to the processing are so significant that the processing becomes completely different in nature to what it was before. WP29 emphasises that all of the other rules in the GDPR, including those relating to incompatible further processing, continue to apply irrespective of compliance with the transparency obligations.

資料控管者應仔細考量透明化下所需提供更新資訊的每種情狀和背景，包括變更對當事人的潛在影響以及用於傳達該項變更之方式，並得以證明變更通知和變更生效之間的時間如何符合對當事人之公正原則。此外，WP29的立場為，與公正原則一致，在向當事人通知此類變更時，資料控管者亦應說明該變更對當事人可能產生之影響。然而，符合透明化要件並無法「掩飾」該項運用之重大變更，已導致該運用在本質上已與之前完全不同。WP29強調，GDPR中其他所有的規則，包含與其他運用不相容之相關規則，無論是否符合透明化義務，皆繼續適用。

32. Additionally, even when transparency information (e.g. contained in a privacy statement/ notice) does not materially change, it is likely that data subjects who have been using a service for a significant period of time will not recall the information provided to them at the outset under Articles 13 and/or 14. WP29 recommends that controllers facilitate data subjects to have continuing easy access to the information to re-acquaint themselves with the scope of the data processing. In accordance with the accountability principle, controllers should also consider whether, and at what intervals, it is appropriate for them to provide express reminders to data subjects as to the fact of the privacy statement/ notice and where they can find it.

此外，即使透明化資訊（例如隱私聲明/通知中包含之資訊）並無重大變更，但於長時間使用服務後，當事人已無法回憶起最初依據第13條和/或第14條所提供之資訊。WP29建議控管者應使當事人能持續輕鬆取得該資訊，以便重新了解資料運用之範圍。依據課責性原則，控管者亦應考量是否以及間隔多長時間後，適合明確提醒當事人關於隱私聲明/通知之資訊，及可於何處找到該資訊。

Modalities - format of information provision

提供方式 – 提供資訊之格式

33. Both Articles 13 and 14 refer to the obligation on the data controller to *"provide the data subject with all of the following information..."* The operative word here is "provide". This means that the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.). The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app. The example at paragraph 11 illustrates this point. As noted above at paragraph 17, WP29 recommends that the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (e.g. whether in a digital form on a website or in paper format) which can be easily accessed should they wish to consult the entirety of the information.

第13條和第14條皆提及資料控管者有義務「*向當事人提供以下所有資訊...*」。此處之關鍵詞為「提供」。此意味著資料控管者必須採取積極之步驟向當事人提供相關資訊，或主動將當事人引導至資訊所在位置（例如，透過直接連結，使用QR碼等）。當事人無須主動在其他資訊中（例如網站或應用程式中的使用條款和條件）搜尋這些條款所涵蓋之資訊。相關說明請參閱第11段中之示例。如前文第17段所述，WP29建議，提供予當事人之全部資訊應放置於同一個位置或以一份完整之文件呈現（無論是在網頁上的數位資訊或紙本），使當事人欲查閱整份文件時，即可以輕鬆地取得。

34. There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible. As such, and bearing in mind the fundamental principles of accountability and fairness, controllers must undertake their own analysis of the nature, circumstances, scope and context of the processing of personal data which they carry out and decide, within the legal requirements of the GDPR and taking account of the recommendations in these Guidelines particularly at paragraph 36 below, how to prioritise information which must be provided to data subjects and what are the appropriate levels of detail and methods for conveying the information.

GDPR的規範存在著本質上的緊張關係，一方面GDPR要求向當事人提供全面性之資訊，另一方面要求以簡潔、透明、易懂且便於取得之形式為之。因此，控管者應本於課責性和公正性的基本原則，就其執行及決定個人資料運用之本質、情況、範圍和背景自行分析，於GDPR的法律要求範圍內並考量本指引中之建議(特別是第36段)，決定必須提供予當事人資訊之優先順序，以及傳達資訊的適當詳細程度和方式。

Layered approach in a digital environment and layered privacy statements/ notices

數位環境中之分層方式和分層隱私聲明/通知

35. In the digital context, in light of the volume of information which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue. Layered privacy statements/ notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/ notice that they wish to read. It should be noted that layered privacy statements/ notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/ notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/ how they can find that detailed information within the layers of the privacy statement/ notice. It is also important that the information contained within the different layers of a layered notice is consistent and that the layers do not provide conflicting information.

在數位環境中，考量到需要提供給當事人之資訊量，資料控管者在選擇使用各種方式之組合來確保透明化時，可採用分層方式。WP29特別建議，分層隱私聲明/通知應使用連結方式，至須提供給當事人之各類資訊，而非僅在螢幕上單一通知中顯示所有相關資訊，以避免資訊疲勞。分層隱私聲明/通知有助於解決完整性和理解性間之緊張關係，特別是可引導用戶直接到所欲閱讀之聲明/通知部分。另應注意，分層隱私聲明/通知並非須經多次點擊始能獲得相關資訊之嵌套頁面（nested pages）。隱私聲明/通知的第一層設計和版面，應使當事人能就運用其個人資料可取得之相關資訊有清楚之概觀，以及在何處/如何於隱私聲明/通知的各個階層中找到詳細資訊。同等重要者為，於分層通知中不同層級所包含之資訊須具有一致性，且不應提供相衝突之資訊。

36. As regards the content of the first modality used by a controller to inform data subjects in a layered approach (in other words the primary way in which the controller first engages with a data subject), or the content of the first layer of a layered privacy statement/ notice, WP29 recommends that the first layer/ modality should include the details of the purposes of processing, the identity of controller and a description of the data subject's rights. (Furthermore this information should be directly brought to the attention of a data subject at the time of collection of the personal data e.g. displayed as a data subject fills in an online form.) The importance of providing this information upfront arises in particular from Recital

39.[34] While controllers must be able to demonstrate accountability as to what further information they decide to prioritise, WP29's position is that, in line with the fairness principle, in addition to the information detailed above in this paragraph, the first layer/ modality should also contain information on the processing which has the most impact on the data subject and processing which could surprise them. Therefore, the data subject should be able to understand from information contained in the first layer/ modality what the consequences of the processing in question will be for the data subject (see also above at paragraph 10).

WP29於控管者以分層方式通知當事人之第一種形式內容(亦即控管者首次與當事人接觸之主要方式），或分層隱私聲明/通知第一層之內容，建議第一層/形式應包含運用目的之詳細資訊、控管者之身分和當事人權利之描述。（此外，該資訊應在蒐集個人資料時直接引起當事人之注意，例如，於當事人填寫網路表格時顯示。）前言第39點尤其強調預先提供該資訊之重要性。[34] 雖然控管者基於課責性必須能夠證明其如何決定資訊之優先性，但WP29之立場為，依據公正原則，除本段以上詳述之資訊外，第一層/形式亦應包含對當事人產生重大影響或使其感到意外之運用的相關資訊。因此，當事人應能夠從第一層/形式包含之資訊中理解相關之資料運用將對其產生之後果（亦請參閱前文第10段）。

37. In a digital context, aside from providing an online layered privacy statement/ notice, data controllers may also choose to use *additional* transparency tools (see further examples considered below) which provide tailored information to the individual data subject which is specific to the position of the individual data subject concerned and the goods/ services which that data subject is availing of. It should be noted however that while WP29 recommends the use of online layered privacy statements/ notices, this recommendation does not exclude the development and use of other innovative methods of compliance with transparency requirements.

在數位環境中，除了提供網路的分層隱私聲明/通知外，資料控管者亦可選擇使用*其他*透明化工具（請參閱以下其他示例），為個別當事人就其關切之特定位置以及所使用之商品/服務，提供客製化之資訊。然而，應需注意，雖然WP29建議使用網路的分層隱私聲明/通知，但該建議並不排除發展和使用其他符合透明化要求之創新方式。

Layered approach in a non-digital environment

[34] Recital 39 states, on the principle of transparency, that "That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed."
透明化原則，前言第39點指出，「該原則特別涉及應提供給當事人關於控管者身分和運用目的之資訊，以及用於確保對相關自然人資料運用之公正與透明化，並確保當事人有權利就其所被運用之個人資料進行確認和溝通。」

非數位環境下之分層方式

38. A layered approach to the provision of transparency information to data subjects can also be deployed in an offline/ non-digital context (i.e. a real-world environment such as person-to-person engagement or telephone communications) where multiple modalities may be deployed by data controllers to facilitate the provision of information. (See also paragraphs 33 to 37 and 39 to 40 in relation to different modalities for providing the information.) This approach should not be confused with the separate issue of layered privacy statements/ notices. Whatever the formats that are used in this layered approach, WP29 recommends that the first "layer" (in other words the primary way in which the controller first engages with the data subject) should generally convey the most important information (as referred to at paragraph 36 above), namely the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject. For example, where the first point of contact with a data subject is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13/ 14 by way of further, different means, such as by sending a copy of the privacy policy by email and/ or sending the data subject a link to the controller's layered online privacy statement/ notice.

以分層方式向當事人提供之透明化資訊亦可使用於離線/非數位環境中（即真實世界環境，例如人對人交流或電話溝通），資料控管者可使用不同類型之方式，以便於提供資訊。（有關提供資訊之不同方式，請另參閱第33至37段和第39至40段。）然不應將此模式與分層隱私聲明/通知之個別問題相混淆。無論在此種分層方式中使用何種格式，WP29建議第一「層」（亦即控管者首次與當事人接觸之主要方式）通常應傳達最重要之資訊（如上文第36段所述），即運用目的之細節、控管者之身分和當事人所擁有之權利，以及運用產生之最大影響或可能使當事人感到意外之運用。例如，第一次與當事人係透過電話聯繫，則可在與當事人通話期間提供此類資訊，並可透過進一步且不同之方式，權衡第13/14條之要求，向其提供相關資訊，例如透過電子郵件傳送隱私政策副本和/或寄送控管者網路分層隱私聲明/通知之連結予當事人。

"Push" and "pull" notices

「推播」和「索取」式通知

39. Another possible way of providing transparency information is through the use of "push" and "pull" notices. Push notices involve the provision of "just-in-time" transparency information notices while "pull" notices facilitate access to information by methods such as permission management, privacy dashboards and "learn more" tutorials. These allow for a more user-

centric transparency experience for the data subject.

另一種提供透明化資訊可能之方式為使用「推播」和「索取」式通知。推播通知涉及提供「即時」透明資訊通知，而「索取」通知則透過如權限管理、隱私面板和「了解更多」等方式便利資訊之取得。這些方式為當事人提供了更加以用戶為中心之透明化體驗。

- A privacy dashboard is a single point from which data subjects can view 'privacy information' and manage their privacy preferences by allowing or preventing their data from being used in certain ways by the service in question. This is particularly useful when the same service is used by data subjects on a variety of different devices as it gives them access to and control over their personal data no matter how they use the service. Allowing data subjects to manually adjust their privacy settings via a privacy dashboard can also make it easier for a privacy statement/ notice to be personalised by reflecting only the types of processing occurring for that particular data subject. Incorporating a privacy dashboard into the existing architecture of a service (e.g. by using the same design and branding as the rest of the service) is preferable because it will ensure that access and use of it will be intuitive and may help to encourage users to engage with this information, in the same way that they would with other aspects of the service. This can be an effective way of demonstrating that 'privacy information' is a necessary and integral part of a service rather than a lengthy list of legalese.

  隱私面板是一個單一接觸點，當事人可查看「隱私資訊」並藉由允許或防止相關服務以特定方式運用其資料管理其隱私偏好選項。若當事人在各種不同設備上使用相同服務時，此方式特別有效，因無論其如何使用該服務，皆可控制自身之個人資料。允許當事人透過隱私面板自行手動調整其隱私設定亦可反映針對該特定當事人而發生之運用類型，以使隱私聲明/通知更加個人化。將隱私面板整合至現有服務架構中（例如，透過使用與其他服務相同之設計和品牌）應屬首選，因為如此可確保面板之造訪和使用具有直觀性，且可有助於鼓勵用戶參與這些資訊，如同參與其他服務一般。此為一種有效的方式以證明「隱私資訊」係服務必要和不可或缺之一部分，而非冗長之法律術語列表。

- A just-in-time notice is used to provide specific 'privacy information' in an ad hoc manner, as and when it is most relevant for the data subject to read. This method is useful for providing information at various points throughout the process of data collection; it helps to spread the provision of information into easily digestible chunks and reduces the reliance on a single privacy statement/ notice containing information that is difficult to understand out of context. For example, if a data subject purchases a product online, brief explanatory information can be provided in pop-ups accompanying relevant fields of text. The information next to a field requesting the data subject's telephone number could explain for example that this data is only being collected for the purposes of contact regarding the purchase and that it will only be disclosed to the delivery service.

即時通知係當與當事人最為相關之訊息需要其讀取時，以特別的方式提供特定之「隱私資訊」。此方式對於在整個資料蒐集過程中的各個時點提供資訊十分有用；該方式有助於將資訊之提供分散至易於瞭解之區塊，並減少對包含難以理解的關聯資訊之單一隱私聲明/通知的依賴。例如，若當事人於網路購買產品，則可在伴隨相關文字的彈出視窗中提供簡要之解釋性資訊。請求當事人提供電話號碼的文字旁即可說明例如「僅為與該購買相關之聯絡目的而蒐集該資料，且該資料僅會於遞送服務時揭露」。

Other types of "appropriate measures"

其他類型之「適當措施」

40. Given the very high level of internet access in the EU and the fact that data subjects can go online at any time, from multiple locations and different devices, as stated above, WP29's position is that an "appropriate measure" for providing transparency information in the case of data controllers who maintain a digital/ online presence, is to do so through an electronic privacy statement/ notice. However, based on the circumstances of the data collection and processing, a data controller may need to additionally (or alternatively where the data controller does not have any digital/online presence) use other modalities and formats to provide the information. Other possible ways to convey the information to the data subject arising from the following different personal data environments may include the following modes applicable to the relevant environment which are listed below. As noted previously, a layered approach may be followed by controllers where they opt to use a combination of such methods while ensuring that the most important information (see paragraph 36 and 38) is always conveyed in the first modality used to communicate with the data subject.

有鑑於歐盟網路使用之高普及性，以及當事人可隨時從多個地點和不同設備連接至網路，如上所述，WP29之立場為，若在資料控管者設有數位/網路平台之情況下，提供透明化資訊之「適當措施」應透過電子隱私聲明/通知為之。然而，基於資料蒐集和運用之情狀，資料控管者可能需要另外（或在資料控管者不擁有任何數位/網路平台之情況下）使用其他方式和格式來提供資訊。其他因以下不同之個人資料情境可能向當事人傳達資訊之方式，可能包含可適用於以下所列相關情境之模式。如上所述，當控管者選擇組合使用這些方式以確保與當事人的第一種溝通形式傳達最重要之資訊(請參閱第36、38段)時，其可能使用分層方式為之。

a. Hard copy/ paper environment, for example when entering into contracts by postal means: written explanations, leaflets, information in contractual documentation, cartoons, infographics or flowcharts;

書面/紙本情境，例如透過郵寄方式簽訂契約時：書面說明、傳單、契約文件中之資訊、漫畫、資訊圖表或流程圖；

b. Telephonic environment: oral explanations by a real person to allow interaction and questions to be answered or automated or pre-recorded information with options to hear further more detailed information;
電話情境：由真人口頭說明，藉由互動和提問得到解答，或以自動或預先錄製之資訊，提供聽取更多詳細資訊之選項；

c. Screenless smart technology/ IoT environment such as Wi-Fi tracking analytics: icons, QR codes, voice alerts, written details incorporated into paper set-up instructions, videos incorporated into digital set-up instructions, written information on the smart device, messages sent by SMS or email, visible boards containing the information, public signage or public information campaigns;
無螢幕智能技術/物聯網情境，如Wi-Fi追蹤分析：圖示、QR碼、語音警示、併入紙本安裝指引中之詳細說明、數位安裝指引中之影音、智能設備上之書面資訊、透過短訊或電子郵件發送之資訊、顯示板包含之資訊、公共看板或公共資訊活動；

d. Person to person environment, such as responding to opinion polls, registering in person for a service: oral explanations or written explanations provided in hard or soft copy format;
面對面之情境，例如回應民意調查或親自申請相關服務：口頭說明或以紙本或電子格式提供書面說明；

e. "Real-life" environment with CCTV/ drone recording: visible boards containing the information, public signage, public information campaigns or newspaper/ media notices.
CCTV /無人機錄製之「即時」情境：顯示板包含之資訊、公共看板、公共資訊活動或報紙/媒體通知。

Information on profiling and automated decision-making
有關資料剖析和自動決策之資訊

41. Information on the existence of automated decision-making, including profiling, as referred to in Articles 22.1 and 22.4, together with meaningful information about the logic involved and the significant and envisaged consequences of the processing for the data subject, forms part of the obligatory information which must be provided to a data subject under Articles 13.2(f) and 14.2(g). WP29 has produced guidelines on automated individual decision-making and profiling[35] which should be referred to for further guidance on how transparency should be given effect in the particular circumstances of profiling. It should be noted that, aside from the specific transparency requirements applicable to automated decision-making under Articles 13.2(F) and 14.2(g), the comments in these guidelines relating to the importance of informing data subjects as to the consequences of processing of their personal data, and the general principle that data subjects should not be taken by surprise by the processing of their personal

data, equally apply to profiling generally (not just profiling which is captured by Article 22[36]), as a type of processing.[37]

第22條第1項和第22條第4項所述之現存自動決策資訊（包括資料剖析）、與所涉邏輯相關之有意義資訊，及運用對當事人產生重大和預設之後果，皆構成依據第13條第2項第f款和14條第2項第g款中必須向當事人提供之強制資訊之一部分。WP29制定了關於自動化個人決策和資料剖析之指引[35]，針對特定資料剖析時如何實現透明化，應進一步參考這些指引。應注意的是，除依第13條第2項第f款和第14條第2項第g款規定之自動決策應適用的具體透明化要件外，這些指引中有關通知當事人運用其個人資料後果之重要性的評論，以及當事人不應就運用其個人資料而感到意外之一般原則，同樣普遍適用於資料剖析之情況（不僅限於第22條所涵蓋之剖析[36]），因其亦屬資料運用類型之一。[37]

Other issues – risks, rules and safeguards

其他議題 - 風險、規則和安全維護措施

42. Recital 39 of the GDPR also refers to the provision of certain information which is not explicitly covered by Articles 13 and Article 14 (see recital text above at paragraph 28). The reference in this recital to making data subjects aware of the risks, rules and safeguards in relation to the processing of personal data is connected to a number of other issues. These include data protection impact assessments (DPIAs). As set out in the WP29 Guidelines on DPIAs,[38] data controllers may consider publication of the DPIA (or part of it), as a way of fostering trust in the processing operations and demonstrating transparency and accountability, although such publication is not obligatory. Furthermore, adherence to a code of conduct (provided for under Article 40) may go towards demonstrating transparency, as codes of conduct may be drawn up for the purpose of specifying the application of the GDPR with regard to: fair and transparent processing; information provided to the public and to data subjects; and information provided to, and the protection of, children, amongst other issues.

GDPR前言第39點亦提及某些第13條、第14條未明確涵蓋之應提供資訊（請參閱前文第28段前言文字）。該前言指出使當事人了解與個人資料運用相關之風險、規則和安全維護措施亦與其他議題有所關聯。其中包含個資保護影響評估（DPIAs）。如WP29關於DPIA之指引所述，[38] 資料控管者可考慮公佈DPIA（或其中一部分），作為促進對運用作業之

[35] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251

WP 251，第2016/679號規則，關於自動化個人決策和資料剖析指引，。

[36]This applies to decision-making based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her.

此條款適用於僅基於自動化運用（包括剖析）對有關當事人產生法律效果或類似重大影響之決策。

[37] Recital 60, which is relevant here, states that "Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling".

前言第60點就此相關之部分指出，「此外，當事人應被告知資料剖析之存在以及該剖析之後果」。

[38] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a

信任，並做為展現透明化和課責性的一種方式，雖然此類公佈非屬強制性。此外，遵守行為守則（依據第40條之規定）可用於證明透明化，因行為守則可能就是以適用下列GDPR相關規範為目的所草擬：公正透明之運用；向公眾和當事人提供資訊；向兒童提供資訊以及保護等議題。

43. Another relevant issue relating to transparency is data protection by design and by default (as required under Article 25). These principles require data controllers to build data protection considerations into their processing operations and systems from the ground up, rather than taking account of data protection as a last-minute compliance issue. Recital 78 refers to data controllers implementing measures that meet the requirements of data protection by design and by default including measures consisting of transparency with regard to the functions and processing of personal data.

與透明化相關之另一議題為資料保護設計（by design）和預設（by default）（依據第25條之要求）。這些原則要求資料控管者從一開始便將資料保護考量納入其運用作業和系統，而非將資料保護視為最後的法遵議題。前言第78點指出資料控管者應執行符合設計及預設資料保護要求之措施，包含與個人資料之功能和運用相關之透明化措施。

44. Separately, the issue of joint controllers is also related to making data subjects aware of the risks, rules and safeguards. Article 26.1 requires joint controllers to determine their respective responsibilities for complying with obligations under the GDPR in a transparent manner, in particular with regard to the exercise by data subjects of their rights and the duties to provide the information under Articles 13 and 14. Article 26.2 requires that the essence of the arrangement between the data controllers must be made available to the data subject. In other words, it must be completely clear to a data a subject as to which data controller he or she can approach where they intend to exercise one or more of their rights under the GDPR.[39]

此外，共同控管者的議題亦與使當事人知悉風險、規則和安全維護措施相關。第26條第1項要求共同控管者以透明之方式確認各自履行GDPR所定義務之責任，尤其是關於當事人行使其權利及依據第13條和第14條所需提供資訊之義務。第26條第2項要求資料控管者間之實質安排必須提供予當事人。易言之，若當事人欲行使其在GDPR下之一項或多項權利時，該當事人必須清楚知道應聯繫何資料控管者。[39]

Information related to further processing

與進階運用相關之資訊

---

high risk" for the purposes of Regulation 2016/679, WP 248 rev.1

WP 248 rev.1，第2016/679號規則有關個資保護影響評估（DPIA）指引和確認運用是否「可能造成高風險」。

[39] Under Article 26.3, irrespective of the terms of the arrangement between joint data controllers under Article 26.1, a data subject may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.

依據第26條第3項，不論第26條第1項規定之共同資料控管者間之安排條件為何，當事人可依據GDPR對任一共同資料控管者行使其權利。

45. Both Articles 13 and Article 14 contain a provision[40] that requires a data controller to inform a data subject if it intends to further process their personal data for a purpose other than that for which it was collected/ obtained. If so, *"the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2".* These provisions specifically give effect to the principle in Article 5.1(B) that personal data shall be collected for specified, explicit and legitimate purposes, and further processing in a manner that is *incompatible* with these purposes is prohibited.[41] The second part of Article 5.1(B) states that further processing for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes, shall, in accordance with Article 89.1, not be considered to be incompatible with the initial purposes. Where personal data are further processed for purposes that are *compatible* with the original purposes (Article 6.4 informs this issue[42]), Articles 13.3 and 14.4 apply. The requirements in these articles to inform a data subject about further processing promotes the position in the GDPR that a data subject should reasonably expect that at the time and in the context of the collection of personal data that processing for a particular purpose may take place.[43] In other words, a data subject should not be taken by surprise at the purpose of processing of their personal data.

第13條和第14條皆規定[40]，若資料控管者欲進階運用個人資料之目的不同於蒐集/取得該資料之原始目的時，必須通知當事人。若為此情況，「*控管者在進階運用之前，應提供當事人有關該其他目的之資訊以及第2項所述之任何相關進階資訊*」。這些規定具體實現第5條第1項第b款規定，蒐集個人資料之目的應特定、明確及合法，且不得以*不符合*該等目的之方式做進階運用之原則。[41] 第5條第1項第b款第二部分規定，當進階運用係基於公共利益之歸檔目的、科學或歷史研究目的或統計目的，則依第89條第1項規定，不應視為不符合原始目的。當進階運用個人資料*符合*原始目的時（第6條第4項說明此議題[42]），適用第13條第3項和第14條第4項之規定。這些條款規定向當事人提供有關進階運用資訊

[40] At Articles 13.3 and 14.4, which are expressed in identical terms, apart from the word "collected", which is used in Article 13, and which is replaced with the word "obtained" in Article 14.
第13條第3項和第14條第4項使用相同之術語表達，除第13條中使用「蒐集」一詞，而第14條中以「取得」一詞替代。

[41] See, for example on this principle, Recitals 47, 50, 61, 156, 158; Articles 6.4 and 89
該原則之示例請參閱前言第47、50、61、156、158點；第6條第4項和89條。

[42] Article 6.4 sets out, in non-exhaustive fashion, the factors which are to be taken into account in ascertaining whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, namely: the link between the purposes; the context in which the personal data have been collected; the nature of the personal data (in particular whether special categories of personal data or personal data relating to criminal offences and convictions are included); the possible consequences of the intended further processing for data subjects; and the existence of appropriate safeguards.
第6條第4項以非完全列舉之方式規定在確認用於其他目的之運用是否與最初收蒐集個人資料之目的相符時所應考量之因素，即：目的間之關聯；蒐集個人資料之背景；個人資料之性質（尤其是特殊類型之個人資料或個人資料與刑事前科和犯罪相關聯時）；進階運用對當事人可能造成之後果；以及是否存在適當安全維護措施。

之要求，體現了在GDPR下當事人應得合理期待在蒐集個人資料時或過程中，皆係基於特定目的之運用。[43] 換言之，當事人不應就運用其個人資料之目的而感到意外。

46. Articles 13.3 and 14.4, insofar as they refer to the provision of *"any relevant further information as referred to in paragraph 2",* may be interpreted at first glance as leaving some element of appreciation to the data controller as to the extent of and the particular categories of information from the relevant sub-paragraph 2 (i.e. Article 13.2 or 14.2 as applicable) that should be provided to the data subject. (Recital 61 refers to this as "*other necessary information*".) However the default position is that all such information set out in that sub-article should be provided to the data subject unless one or more categories of the information does not exist or is not applicable.

由於第13條第3項和14條第4項規定「*第2項所述之任何相關進階資訊*」，初看可解釋為該條款就第13條第2項或14條第2項第2款應提供予當事人之相關資訊的程度和特定種類，為控管者留有評估之空間。（前言第61點將此類資訊稱為「*其他必要資訊*」。）然而，預設之立場為該款所列之所有資訊，除有一種或多種資訊不存在或不適用之情形外，皆應提供予當事人。

47. WP29 recommends that, in order to be transparent, fair and accountable, controllers should consider making information available to data subjects in their privacy statement/ notice on the compatibility analysis carried out under Article 6.4[44] where a legal basis other than consent or national/ EU law is relied on for the new processing purpose. (In other words, an explanation as to how the processing for the other purpose(s) is compatible with the original purpose). This is to allow data subjects the opportunity to consider the compatibility of the further processing and the safeguards provided and to decide whether to exercise their rights e.g. the right to restriction of processing or the right to object to processing, amongst others.[45] Where controllers choose not to include such information in a privacy notice/ statement, WP29 recommends that they make it clear to data subjects that they can obtain the information on request.

WP29建議，為符合透明、公正和課責義務，當新的運用目的之法律依據並非來自於同意或國家/歐盟法律，控管者應考量在其隱私聲明/通知中向當事人提供有關依據第6條第4項[44]所為之兼容性分析資訊。（換言之，關於其他運用目的與原始目的相容之解釋）。旨在使當事人有機會考量進階運用之兼容性和所提供之安全維護措施，並決定是否行使其權利，例如：限制運用之權利或拒絕運用之權利等。[45] 若控管者選擇不在隱私通知/

[43] Recitals 47 and 50
前言第47和50點。
[44] Also referenced in Recital 50
另參考前言第50點。
[45] As referenced in Recital 63, this will enable a data subject to exercise the right of access in order to be aware of and

聲明中提供此類資訊，WP29建議其向當事人明確表明可依據請求取得資訊。

48. Connected to the exercise of data subject rights is the issue of timing. As emphasised above, the provision of information in a timely manner is a vital element of the transparency requirements under Articles 13 and 14 and is inherently linked to the concept of fair processing. Information in relation to *further processing* must be provided "prior to that further processing". WP29's position is that a reasonable period should occur between the notification and the processing commencing rather than an immediate start to the processing upon notification being received by the data subject. This gives data subjects the practical benefits of the principle of transparency, allowing them a meaningful opportunity to consider (and potentially exercise their rights in relation to) the further processing. What is a reasonable period will depend on the particular circumstances. The principle of fairness requires that the more intrusive (or less expected) the further processing, the longer the period should be. Equally, the principle of accountability requires that data controllers be able to demonstrate how the determinations they have made as regards the timing for the provision of this information are justified in the circumstances and how the timing overall is fair to data subjects. (See also the previous comments in relation to ascertaining reasonable timeframes above at paragraphs 30 to 32.)

與當事人權利行使相關者為時間點之問題。如上所述，及時提供資訊是第13條和第14條透明化要求下的一個重要條件，本質上並與公正運用之概念相關。與*進階運用*相關之資訊必須在「進階運用前」提供。WP29之立場為，在通知和開始運用間應存在合理期間，即不得在當事人收到通知後立即開始運用。此為透明化原則給予當事人之實質效益，使其有機會就進階運用做有意義的思考（並可能行使與進階運用相關之權利）。合理期間之範圍取決於具體情狀。公正性原則要求當進階運用越具侵害性（或較難預期），期間應越長。同樣，課責性原則要求資料控管者能夠證明，在該情境下提供該資訊的時間相關之決策於此種情狀下為合理的，以及整體時間之決策對當事人係公正的。（請另參閱上文第30至32段關於確認合理期間之意見。）

Visualisation tools

視覺化工具

49. Importantly, the principle of transparency in the GDPR is not limited to being effected simply through language communications (whether written or oral). The GDPR provides for visualisation tools (referencing in particular, icons, certification mechanisms, and data protection seals and marks) where appropriate. Recital 58[46] indicates that the accessibility of information addressed to the public or to data subjects is especially important in the online

to verify the lawfulness of the processing.

如前言第63點所述，如此將使當事人得行使其近用權以了解並檢視運用之合法性。

environment.[47]

重要的是，GDPR下之透明化原則不僅限於透過語言溝通（書面或口頭）而實現。GDPR規定在適當情況下可提供視覺化之工具(特別是圖示、認證機制和資料保護標章和標誌)。前言第58點[46]指出，在網路環境中，向公眾或當事人傳達資訊的可得性尤為重要。[47]

Icons

圖示

50. Recital 60 makes provision for information to be provided to a data subject "in combination" with standardised icons, thus allowing for a multi-layered approach. However, the use of icons should not simply replace information necessary for the exercise of a data subject's rights nor should they be used as a substitute to compliance with the data controller's obligations under Articles 13 and 14. Article 12.7 provides for the use of such icons stating that:
前言第60點指出提供予當事人之資訊可與標準化圖示「組合」，從而允許多層次之方式。然而，圖示之使用不應替代當事人行使權利所必需之資訊，亦不應作為資料控管者符合第13條和第14條所定義務之替代。第12條第7項規定使用此類圖示之情況：

> "*The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where icons are presented electronically they shall be machine-readable*".
> 「*依據第13條和第14條提供予當事人之資訊，可與標準化圖示組合使用，以便提供易見、易懂且清晰易讀之方式，並就預計之運用提出有意義之概述。當圖示係以電子方式呈現時，應使用機器可讀取之方式。*」

51. As Article 12.7 states that *"Where the icons are presented electronically, they shall be machine- readable",* this suggests that there may be situations where icons are not presented electronically,[48] for example icons on physical paperwork, IoT devices or IoT device packaging, notices in public places about Wi-Fi tracking, QR codes and CCTV notices.
如第12條第7項所述「*當圖示係以電子方式呈現時，應使用機器可讀取之方式*」，這表示可能存在圖示非以電子方式呈現之情況，[48]例如圖示標示於實體文書上、於物聯網設備

---

[46] "Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising."
「此類資訊可使用電子形式提供，例如當透過網站向公眾傳達資訊。尤其在行為者眾多且實務技術複雜之情形下，會造成當事人難以知悉並理解其個人資料是否、由誰、以何目的被蒐集，例如網路廣告之情形。」

[47] In this context, controllers should take into account visually impaired data subjects (e.g. red-green colour blindness).
於此情形下，控管者應考量視覺受損之當事人（例如紅綠色盲）。

[48] There is no definition of "machine-readable" in the GDPR but Recital 21 of Directive 2013/37/EU17 defines "machine- readable" as:
GDPR中並無「機器可讀取」之定義，但第2013/37 / EU17號指令前言第21點將「機器可讀取」定義為：

或物聯網設備包裝上、公共場所關於Wi-Fi追蹤之通知上、於QR碼和CCTV之通知上。

52. Clearly, the purpose of using icons is to enhance transparency for data subjects by potentially reducing the need for vast amounts of written information to be presented to a data subject. However, the utility of icons to effectively convey information required under Articles 13 and 14 to data subjects is dependent upon the standardisation of symbols/ images to be universally used and recognised across the EU as shorthand for that information. In this regard, the GDPR assigns responsibility for the development of a code of icons to the Commission but ultimately the European Data Protection Board may, either at the request of the Commission or of its own accord, provide the Commission with an opinion on such icons.[49] WP29 recognises that, in line with Recital 166, the development of a code of icons should be centered upon an evidence-based approach and in advance of any such standardisation it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in this context.

顯然地，使用圖示之目的在透過可能地減少向當事人呈現大量書面資訊之需要來增強對當事人之透明化。然而，圖示能否有效地將第13條和第14條所要求之資訊傳達予當事人，取決於該符號/圖像之標準化是否在歐盟境內被普遍使用和承認作為相關資訊之簡化圖示。有鑑於此，GDPR將制定圖示代碼之責任交予執委會，但最終歐洲個人資料保護委員會（EDPB）可應執委會之要求，或自行向執委會提供有關此類圖示之意見。[49] WP29認為，與前言第166點一致，圖示代碼之建立應以循證方式為中心，且為使圖示能有效之使用，於標準化之前，有必要與產業和廣泛大眾一起進行大規模之研究。

"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."

「一種文件格式，使軟體應用程式可輕鬆確認、識別和提取特定資料，包括各別事實陳述及其內部結構。以機器可讀取格式建立之文件中所編碼之資料屬於機器可讀取之資料。機器可讀取格式可以是開放或專有的；其可為正式或非正式之標準。若以限制自動運用文件格式編碼之文檔，因不得或不易從中提取資料，所以不應視為係機器可讀取之格式。成員國應酌情鼓勵使用開放、機器可讀取之格式。」

[49] Article 12.8 provides that the Commission is empowered to adopt delegated acts under Article 92 for the purpose of determining the information to be presented by the icons and the information for providing standardised icons. Recital 166 (which deals with delegated acts of the Commission in general) is instructive, providing that the Commission must carry out appropriate consultations during its preparatory work, including at expert level. However, the European Data Protection Board (EDPB) also has an important consultative role to play in relation to the standardisation of icons as Article 70.1(r) states that the EDPB shall on its own initiative or, where relevant, at the request of the Commission, provide the Commission with an opinion on icons.

第12條第8項規定，執委會有權依據第92條委託，以確認圖示所呈現之資訊和提供標準化圖示之資訊。具有指導意義之前言第166點（有關執委會一般之委託行為）指出，執委會在籌備工作期間，必須進行包括專家層級之適當諮詢。然而，歐洲個人資料保護委員會（EDPB）在圖示標準化上也扮演重要的諮詢角色，因第70條第1項第r款規定，EDPB應主動或在相關的情況下應執委會要求，向執委會提供關於圖示之意見。

Certification mechanisms, seals and marks

認證機制、標章和標誌

53. Aside from the use of standardised icons, the GDPR (Article 42) also provides for the use of data protection certification mechanisms, data protection seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by data controllers and processors and enhancing transparency for data subjects.[50] WP29 will be issuing guidelines on certification mechanisms in due course.

除使用標準化圖示外，GDPR（第42條）亦規定使用資料保護認證機制、資料保護標章和標誌，以證明資料控管者和受託運用者符合GDPR運用作業規範，並提高對當事人之透明化。[50] WP29將在適當時機公布認證機制指引。

Exercise of data subjects' rights

當事人權利之行使

54. Transparency places a triple obligation upon data controllers insofar as the rights of data subjects under the GDPR are concerned, as they must:[51]

就GDPR下當事人之權利而言，透明化對資料控管者課予三重義務，因其必須：[51]

- provide information to data subjects on their rights[52] (as required under Articles 13.2(B) and 14.2(c));

  向當事人提供有關其權利之資訊[52]（依據第13條第2項第b款和14條第2項第c款之要求）；

- comply with the principle of transparency (i.e. relating to the quality of the communications as set out in Article 12.1) when communicating with data subjects in relation to their rights under Articles 15 to 22 and 34; and

  在與當事人就第15條至第22條和第34條下之權利進行溝通時需遵守透明化原則（即關於第12條第1項規定之溝通品質）；以及

- facilitate the exercise of data subjects' rights under Articles 15 to 22.

  促進第15至22條當事人權利之行使。

55. The GDPR requirements in relation to the exercise of these rights and the nature of the information required are designed to *meaningfully position* data subjects so that they can vindicate their rights and hold data controllers accountable for the processing of their personal

[50] See the reference in Recital 100

請參閱前言第100點。

[51] Under the Transparency and Modalities section of the GDPR on Data Subject Rights (Section 1, Chapter III, namely Article 12)

依據GDPR關於當事人權利之透明化和形式章節（第1節，第3章，即第12條）。

[52] Access, rectification, erasure, restriction on processing, object to processing, portability

近用、改正、刪除、限制運用、拒絕運用、可攜。

data. Recital 59 emphasises that *"modalities should be provided for facilitating the exercise of the data subject's rights"* and that the data controller should *"also provide means for requests to be made electronically, especially where personal data are processed by electronic means"*. The modality provided by a data controller for data subjects to exercise their rights should be appropriate to the context and the nature of the relationship and interactions between the controller and a data subject. To this end, a data controller may wish to provide one or more different modalities for the exercise of rights that are reflective of the different ways in which data subjects interact with that data controller.

GDPR關於當事人權利之行使和所需提供資訊之本質係為*有意義地定位*當事人，以使其維護自身權利並使資料控管者就其個人資料之運用負責。前言第59點強調「*應提供有利當事人行使其權利之形式*」，且資料控管者「*亦應提供以電子化請求之方式，特別是在透過電子方式運用個人資料時*」。資料控管者為當事人提供行使其權利之形式應符合控管者和當事人間之關聯和互動之本質。為此，資料控管者可能希望提供一種或多種不同行使權利之形式，以對應當事人與其各種互動方式。

Example
示例

A health service provider uses an electronic form on its website, and paper forms in the receptions of its health clinics, to facilitate the submission of access requests for personal data both online and in person. While it provides these modalities, the health service still accepts access requests submitted in other ways (such as by letter and by email) and provides a dedicated point of contact (which can be accessed by email and by telephone) to help data subjects with the exercise of their rights.

醫療衛生服務提供者為便於當事人以網路和當面申請個人資料之近用請求，在其網站上使用電子表格，而在診所服務台使用紙本表格。雖已提供這些型式，但醫療服務仍接受以其他方式（例如透過信件和電子郵件）申請近用請求，並提供專門的聯絡點（可透過電子郵件和電話連絡）以協助當事人行使其權利。

Exceptions to the obligation to provide information
提供資訊義務之例外情形

Article 13 exceptions
第13條之例外情形

56. The only exception to a data controller's Article 13 obligations where it has collected personal data directly from a data subject occurs *"where and insofar as, the data subject already has the*

information".[53] The principle of accountability requires that data controllers demonstrate (and document) what information the data subject already has, how and when they received it and that no changes have since occurred to that information that would render it out of date. Further, the use of the phrase "insofar as" in Article 13.4 makes it clear that even if the data subject has previously been provided with certain categories from the inventory of information set out in Article 13, there is still an obligation on the data controller to supplement that information in order to ensure that the data subject now has a complete set of the information listed in Articles 13.1 and 13.2. The following is a best practice example concerning the limited manner in which the Article 13.4 exception should be construed.

資料控管者第13條義務唯一例外情形為，當直接向當事人蒐集個人資料時，「*在該範圍內，當事人已擁有相關資訊*」[53]。課責性原則要求資料控管者證明（並記錄）當事人已擁有之資訊、取得該資訊之方式和時間以及未發生使該資訊過時之變更。此外，在第13條第4項中使用「就其範圍」一詞清楚表示，即使當事人先前已從第13條規定之資訊清單中取得某些類別之資訊，資料控管者仍有義務補充該資訊，以確保當事人擁有第13條第1項和13條第2項所列舉之完整資訊。以下為第13條第4項例外情形應被有限解釋之最佳實務示例。

Example
示例

An individual signs up to an online email service and receives all of the required Article 13.1 and 13.2 information at the point of sign-up. Six months later the data subject activates a connected instant message functionality through the email service provider and provides their mobile telephone number to do so. The service provider gives the data subject certain Article 13.1 and 13.2 information about the processing of the telephone number (e.g. purposes and legal basis for processing, recipients, retention period) but does not provide other information that the individual already has from 6 months ago and which has not since changed (e.g. the identity and contact details of the controller and the data protection officer, information on data subject rights and the right to complain to the relevant supervisory authority). As a matter of best practice however, the complete suite of information should be provided to the data subject again but the data subject also should be able to easily tell what information amongst it is new. The new processing for the purposes of the instant messaging service may affect the data subject in a way which would prompt them to seek to exercise a right they may have forgotten about, having been informed six months prior. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and their rights.

[53] Article 13.4
第13條第4項。

某當事人註冊網路電子郵件服務，並在註冊時收到第13條第1項和13條第2項規定之所有必要資訊。六個月後，該當事人透過電子郵件服務提供者啟用連結即時訊息功能，並提供其手機號碼。服務提供者向當事人提供依據第13條第1項和13條第2項關於手機號碼運用之資訊（例如運用之目的和法律依據、接收者、保存期限），但未提供當事人於六個月前已獲得且無變更之資訊。（例如控管者和個資保護長之身分和聯絡方式，有關當事人權利之資訊以及向相關監管機關申訴之權利）。然而，最佳實務做法是，應再次向當事人提供整套完整之資訊，但亦應能使當事人輕易辨別其中最新之資訊。此即時訊息服務之新運用行為，可能會促使當事人行使其在六個月前被告知卻可能遺忘之權利。再次提供所有資訊有助於確保當事人充分瞭解其資料被使用之方式和其權利。

Article 14 exceptions

第14條之例外情形

57. Article 14 carves out a much broader set of exceptions to the information obligation on a data controller where personal data has not been obtained from the data subject. These exceptions should, as a general rule, be interpreted and applied narrowly. In addition to the circumstances where the data subject already has the information in question (Article 14.5(A)), Article 14.5 also allows for the following exceptions:

當個人資料並非從當事人取得時，第14條規定了資料控管者提供資訊義務更廣泛之例外情形。作為一般法律規則，這些例外應被狹義地解釋和適用。除當事人已取得相關資訊之情狀（第14條第5項第a款）外，第14條第5項亦允許以下例外情形

- The provision of such information is impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or where it would make the achievement of the objectives of the processing impossible or seriously impair them;

  提供此類資訊係不可能，或不成比例之付出，特別是基於公共利益之歸檔目的、科學或歷史研究目的或統計目的，或其可能造成無法實現運用目的或嚴重損害該目的；

- The data controller is subject to a national law or EU law requirement to obtain or disclose the personal data and that the law provides appropriate protections for the data subject's legitimate interests ; or

  資料控管者取得或揭露個人資料依據成員國法律或歐盟法律之要求，且該法律為當事人之合法利益提供適當之保護；或

- An obligation of professional secrecy (including a statutory obligation of secrecy) which is regulated by national or EU law means the personal data must remain confidential.

依據成員國或歐盟法律規定之職業保密義務（包括法定之保密義務），即個人資料必須保密。

Proves impossible, disproportionate effort and serious impairment of objectives
證明為不可能、不符合比例原則和嚴重損害目的

58. Article 14.5(B) allows for 3 separate situations where the obligation to provide the information set out in Articles 14.1, 14.2 and 14.4 is lifted:
第14條第5項第b款條允許第14條第1項、14條第2項和14條第4項規定所應提供資訊義務之三種各別例外情形：

(i) Where it proves impossible (in particular for archiving, scientific/ historical research or statistical purposes);
當提供資訊被證明係不可能之情形（尤其是基於為歸檔、科學/歷史研究或統計之目的）；

(ii) Where it would involve a disproportionate effort (in particular for archiving, scientific/ historical research or statistical purposes); or
當提供資訊為不成比例之付出（尤其是基於歸檔、科學/歷史研究或統計之目的）；或

(iii) Where providing the information required under Article 14.1 would make the achievement of the objectives of the processing impossible or seriously impair them.
當提供第14條第1項要求之資訊將無法實現運用之目的或嚴重損害該目的。

"Proves impossible"
「證明為不可能」

59. The situation where it "proves impossible" under Article 14.5(B) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus if a data controller seeks to rely on this exemption it must demonstrate the factors that actually *prevent it* from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects. The following example demonstrates this.
第14條第5項第b款中所謂當提供資訊被「證明為不可能」之情形應屬一種可提供全部資訊或完全無法提供資訊之情形，因為不可能是沒有程度上之區分。因此，若資料控管者試圖援用此類例外情形，則必須證明有實際上*阻止其*向當事人提供有關資訊之因素。若在一段期間後，導致「不可能性」之因素已不存在，且可向當事人提供資訊時，資料控管者應立即為之。實際上，僅在少數情況下資料控管者可證明其事實上不可能向當事人

提供資訊。請參閱以下示例。

Example
示例

A data subject registers for a post-paid online subscription service. After registration, the data controller collects credit data from a credit-reporting agency on the data subject in order to decide whether to provide the service. The controller's protocol is to inform data subjects of the collection of this credit data within three days of collection, pursuant to Article 14.3(a). However, the data subject's address and phone number is not registered in public registries (the data subject is in fact living abroad). The data subject did not leave an email address when registering for the service or the email address is invalid. The controller finds that it has no means to directly contact the data subject. In this case, however, the controller may give information about collection of credit reporting data on its website, prior to registration. In this case, it would not be impossible to provide information pursuant to Article 14.

當事人註冊一項後付費線上訂閱服務。註冊後，資料控管者從聯合徵信機構蒐集有關當事人之信用資料，以決定是否提供服務。依據第14條第3項第a款，控管者應在蒐集該信用資料後之三天內通知當事人。然而，當事人之地址和電話號碼並未註冊於公共註冊管理機構（當事人實際上居住於國外）。註冊服務時當事人未留下電子郵件地址或電子郵件地址無效。控管者發現無法直接聯繫當事人。然而，在此情況下，控管者可在註冊之前於其網站上提供關於徵信資料蒐集之資訊。在此情況下，提供第14條規定之資訊並非不可能。

Impossibility of providing the source of the data
無法提供資料來源

60. Recital 61 states that "where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided". The lifting of the requirement to provide data subjects with information on the source of their personal data applies only where this is not possible because different pieces of personal data relating to the same data subject cannot be attributed to a particular source. For example, the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. Given the requirements of data protection by

design and by default,[54] transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organisation can be tracked and traced back to their source at any point in the data processing life cycle (see paragraph 43 above).

前言第61點指出「因使用了各項資料來源，而無法向當事人提供個人資料來源時，應提供一般資訊」。免除向當事人提供關於其個人資料來源資訊之要求，僅適用於因與同一當事人相關之各種個人資料無法追溯至特定來源，而無法提供之情況。例如，資料控管者使用多種來源將多位當事人之個人資料彙集成數據庫，若控管者能夠（雖然耗時或費力）確認個別當事人之個人資料來源，則此一事實尚不足以免除該項要求。有鑑於資料保護設計（by design）和預設（by default）之要求[54]，透明化機制應從底層開始構建至運用系統中，以便組織接收到的所有個人資料皆可在運用過程中的任一時點追蹤和追溯至其來源。（請參閱上文第43段）。

"Disproportionate effort"

「不成比例之付出」

61. Under Article 14.5(B), as with the "proves impossible" situation, "disproportionate effort" may also apply, in particular, for processing *"for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the safeguards referred to in Article 89(1)"*. Recital 62 also references these objectives as cases where the provision of information to the data subject would involve a disproportionate effort and states that in this regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration. Given the emphasis in Recital 62 and Article 14.5(b) on archiving, research and statistical purposes with regard to the application of this exemption, WP29's position is that this exception should not be *routinely* relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes. WP29 emphasises the fact that where these are the purposes pursued, the conditions set out in Article 89.1 must still be complied with and the provision of the information must constitute a disproportionate effort.

依據第14條第5項第b款，與「證明為不可能」之情況相同，「不成比例之付出」亦可適用，特別是當運用係「*基於公共利益之歸檔目的、科學或歷史研究目的或統計目的，且符合第89條第1項之安全維護措施*」。前言第62點亦將這些目的作為向當事人提供資訊不成比例之付出的案例，並指出，應考量當事人之數量、資料之年代和所採行之任何適當安全維護措施。有鑑於前言第62點和第14條第5項第b款強調關於適用此項豁免之歸檔、

[54] Article 25
第25條。

研究和統計目的，WP29之立場為，若資料控管者運用資料之目的並非為了公共利益之歸檔目的、為了科學或歷史研究目的或統計目的，該控管者不應*經常性地*援用此例外情形。WP29強調，即使為這些目的而運用，仍須遵守第89條第1項規定之要件，且提供資訊應達到不成比例之付出。

62. In determining what may constitute either impossibility or disproportionate effort under Article 14.5(B), it is relevant that there are no comparable exemptions under Article 13 (where personal data is collected from a data subject). The only difference between an Article 13 and an Article 14 situation is that in the latter, the personal data is not collected from the data subject. It therefore follows that impossibility or disproportionate effort typically arises by virtue of circumstances which do not apply if the personal data is collected from the data subject. In other words, the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject.
在考量如何構成第14條第5項第b款之「不可能」或「不成比例之付出」時，第13條（從當事人蒐集個人資料）之情形並無與此相當之豁免。第13條和第14條唯一的區別在於，後者之個人資料並非從當事人處蒐集。因此，「不可能」或「不成比例之付出」在通常情況下不適用於從當事人蒐集個人資料之情形。換言之，「不可能」或「不成比例之付出」必須與個人資料並非從當事人取得之事實有直接關聯。

Example
示例

A large metropolitan hospital requires all patients for day procedures, longer-term admissions and appointments to fill in a Patient Information Form which seeks the details of two next-of-kin (data subjects). Given the very large volume of patients passing through the hospital on a daily basis, it would involve disproportionate effort on the part of the hospital to provide all persons who have been listed as next-of-kin on forms filled in by patients each day with the information required under Article 14.
一家綜合醫院要求所有進行日間手術、長期住院和預約之病患填寫病患資料表格，該表格要求填寫兩位近親（當事人）之詳細資訊。由於每天出入醫院病人之數量非常龐大，若要求醫院提供第14條中之資訊給每日被病患在表格上列為近親之所有當事人，對醫院構成不成比例之付出。

63. The factors referred to above in Recital 62 (number of data subjects, the age of the data and any appropriate safeguards adopted) may be indicative of the types of issues that contribute to a data controller having to use disproportionate effort to notify a data subject of the relevant Article 14 information.

前言第62點中提及之因素（當事人之數量、資料之年代和所採行之任何適當安全維護措施）指明某些類型情況可能導致資料控管者必須以不成比例之付出通知當事人第14條相關資訊。

Example
示例

Historical researchers seeking to trace lineage based on surnames indirectly obtain a large dataset relating to 20,000 data subjects. However, the dataset was collected 50 years ago, has not been updated since, and does not contain any contact details. Given the size of the database and more particularly, the age of the data, it would involve disproportionate effort for the researchers to try to trace the data subjects individually in order to provide them with Article 14 information.

歷史研究人員為透過姓氏追溯血緣，間接獲得了與20,000個當事人相關之大型資料集。然而，該資料集係蒐集於50年前，且自此後並無更新，亦不包含任何聯絡方式。鑑於資料集之規模，特別是資料之年代，要求研究人員試著逐一追踪當事人以向其提供第14條之資訊屬不成比例之付出。

64. Where a data controller seeks to rely on the exception in Article 14.5(B) on the basis that provision of the information would involve a disproportionate effort, it should carry out a balancing exercise to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information. This assessment should be documented by the data controller in accordance with its accountability obligations. In such a case, Article 14.5(B) specifies that the controller must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests. This applies equally where a controller determines that the provision of the information proves impossible, or would likely render impossible or seriously impair the achievement of the objectives of the processing. One appropriate measure, as specified in Article 14.5(B), that controllers must always take is to make the information publicly available. A controller can do this in a number of ways, for instance by putting the information on its website, or by proactively advertising the information in a newspaper or on posters on its premises. Other appropriate measures, in addition to making the information publicly available, will depend on the circumstances of the processing, but may include: undertaking a data protection impact assessment; applying pseudonymisation techniques to the data; minimising the data collected and the storage period; and implementing technical and organisational measures to ensure a high level of security. Furthermore, there may be

situations where a data controller is processing personal data which does not require the identification of a data subject (for example with pseudonymised data). In such cases, Article 11.1 may also be relevant as it states that a data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purposes of complying with the GDPR.

當資料控管者因提供資訊將不符合比例原則而欲援用第14條第5項第b款之例外情形時，該控管者應該進行平衡判斷，評估提供資訊所涉及之工作量，以及若未提供該資訊予當事人將對其產生之影響和結果。資料控管者應依據其課責性義務記錄此評估。在此情況下，第14條第5項第b款規定，控管者必須採取適當措施保護當事人之權利、自由和合法利益。此原則亦適用於當控管者確認資訊之提供為不可能時，或可能導致運用目的無法實現或嚴重損害該目的之達成。依據第14條第5項第b款之規定，控管者必須採行的一項適當措施為公開資訊。控管者可透過多種方式達到此目的，例如將資訊放置於網站上、或主動在報紙上宣傳該資訊或在其場所張貼相關資訊海報。除了公開資訊外，其他適當措施將取決於運用之具體情狀，但可包含：踐行個資保護影響評估；使用資料假名化技術；資料蒐集和儲存期之最小化；以及實施技術性和組織性之措施，以確保高度安全保護。此外，資料控管者正在運用的個人資料亦可能不需識別當事人（例如，使用假名化資料）。在此情況下，應考量第11條第1項，該條款規定若僅係為符合GDPR之規範，資料控者並無義務維護、取得或運用其他資訊以識別當事人。

Serious impairment of objectives

對目的之嚴重損害

65. The final situation covered by Article 14.5(B) is where a data controller's provision of the information to a data subject under Article 14.1 is likely to make impossible or seriously impair the achievement of the processing objectives. To rely on this exception, data controllers must demonstrate that the provision of the information set out in Article 14.1 alone would nullify the objectives of the processing. Notably, reliance on this aspect of Article 14.5(B) pre-supposes that the data processing satisfies all of the principles set out in Article 5 and that most importantly, in all of the circumstances, the processing of the personal data is fair and that it has a legal basis.

第14條第5項第b款涵蓋之最後情況為，資料控管者依據第14條第1項向當事人提供資訊可能導致無法達成或嚴重損害該運用目的。欲援用此例外情形，資料控管者必須證明僅提供第14條第1項規定之資訊將使運用之目的無效。另須注意，援用第14條第5項第b款須預先假定資料運用符合第5條規定之所有原則，最為重要者，在所有情狀下，個人資料之運用係公正的，並有法律依據。

Example
示例

Bank A is subject to a mandatory requirement under anti-money laundering legislation to report suspicious activity relating to accounts held with it to the relevant financial law enforcement authority. Bank A receives information from Bank B (in another Member State) that an account holder has instructed it to transfer money to another account held with Bank A which appears suspicious. Bank A passes this data concerning its account holder and the suspicious activities to the relevant financial law enforcement authority. The anti-money laundering legislation in question makes it a criminal offence for a reporting bank to "tip off" the account holder that they may be subject to regulatory investigations. In this situation, Article 14.5(B) applies because providing the data subject (the account holder with Bank A) with Article 14 information on the processing of account holder's personal data received from Bank B would seriously impair the objectives of the legislation, which includes the prevention of "tip-offs". However, general information should be provided to all account holders with Bank A when an account is opened that their personal data may be processed for anti-money laundering purposes.

A銀行為遵守反洗錢法規之強制性要求，必須向相關金融執法機關通報與其持有帳戶有關之可疑活動。A銀行從B銀行（另一個成員國）收到一則資訊，即某帳戶持有人指示B銀行轉賬到A銀行一個看似可疑之賬戶。A銀行將有關其賬戶持有人和可疑活動之資料傳送給相關金融執法機關。相關反洗錢法規規定，若通報銀行「密報」帳戶持有人其可能受到監管調查，則屬於刑事犯罪。此情況適用第14條第5項第b款，因向當事人（A銀行賬戶持有人）提供第14條有關運用從B銀行接收之賬戶持有人個人資料之資訊，將嚴重損害法規之目的，包含妨礙「密報」。然而，在開立賬戶時，A銀行應向所有賬戶持有人提供一般性資訊，告知其個人資料可能運用於反洗錢目的。

Obtaining or disclosing is expressly laid down in law
法律明文規定之取得或揭露

66. Article 14.5(C) allows for a lifting of the information requirements in Articles 14.1, 14.2 and 14.4 insofar as the obtaining or disclosure of personal data *"is expressly laid down by Union or Member State law to which the controller is subject".* This exemption is conditional upon the law in question providing *"appropriate measures to protect the data subject's legitimate interests".* Such a law must directly address the data controller and the obtaining or disclosure in question should be mandatory upon the data controller. Accordingly, the data controller must be able to demonstrate how the law in question applies to them and requires them to either

obtain or disclose the personal data in question. While it is for Union or Member State law to frame the law such that it provides *"appropriate measures to protect the data subject's legitimate interests",* the data controller should ensure (and be able to demonstrate) that its obtaining or disclosure of personal data complies with those measures. Furthermore, the data controller should make it clear to data subjects that it obtains or discloses personal data in accordance with the law in question, unless there is a legal prohibition preventing the data controller from doing so. This is in line with Recital 41 of the GDPR, which states that a legal basis or legislative measure should be clear and precise, and its application should be foreseeable to persons subject to it, in accordance with the case law of the Court of Justice of the EU and the European Court of Human Rights. However, Article 14.5(c) will not apply where the data controller is under an obligation to obtain data *directly from a data subject*, in which case Article 13 will apply. In that case, the only exemption under the GDPR exempting the controller from providing the data subject with information on the processing will be that under Article 13.4 (i.e. where and insofar as the data subject already has the information). However, as referred to below at paragraph 68, at a national level, Member States may also legislate, in accordance with Article 23, for further specific restrictions to the right to transparency under Article 12 and to information under Articles 13 and 14.

若取得或揭露個人資料係「*依據控管者所受拘束之歐盟法律或成員國法律明文規定*」，第14條第5項第c款允許第14條第1項、第2項和第4項所要求提供資訊之免除。此項例外情形是以相關法律須提供「*保護當事人合法利益之適當措施*」為要件。該法律必須直接規範資料控管者，且取得或揭露對資料控管者而言應為強制性。因此，資料控管者必須能證明相關法律之適用，以及該法律如何要求其取得或揭露相關個人資料。雖然歐盟或成員國法律須建構以提供「*保護當事人合法利益之適當措施*」，但資料控管者應確保（並能夠證明）其取得或揭露個人資料係符合此類措施。 此外，除非法律明文禁止，資料控管者應向當事人具體說明其取得或揭露個人資料係根據相關法律規定。此亦符合GDPR前言第41點，該前言指出，依據歐盟法院和歐洲人權法院案例法，法律依據或立法措施應當清楚和明確，且受其拘束之個人應可預見該法律之適用。然而，若資料控管者有義務*直接從當事人取得資料*，在此情況下，適用第13條而不適用第14條第5項第c款。在該情況下，GDPR中唯一得免除控管者向當事人提供相關運用資訊者為第13條第4項之規定（即在該範圍內，當事人已擁有相關資訊）。然而，如下文第68段所述，在國家層級，成員國亦可依據第23條立法，對第12條規定之透明化和第13條和第14條規定之資訊做出進一步具體限制。

Example

示例

A tax authority is subject to a mandatory requirement under national law to obtain the details of employees' salaries from their employers. The personal data is not obtained from the data subjects and therefore the tax authority is subject to the requirements of Article 14. As the obtaining of the personal data by the tax authority from employers is expressly laid down by law, the information requirements in Article 14 do not apply to the tax authority in this instance.

稅務機關必須遵守國家法律強制性之要求，從雇主取得員工薪資詳情。該個人資料並非從當事人取得，因此稅務機關必須符合第14條之要求。由於稅務機關從雇主取得個人資料係法律所明文規定，因此第14條對資訊之要求於此情況下不適用於該稅務機關。

Confidentiality by virtue of a secrecy obligation

保密義務下之機密性

67. Article 14.5(D) provides for an exemption to the information requirement upon data controllers where the personal data "*must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy*". Where a data controller seeks to rely on this exemption, it must be able to demonstrate that it has appropriately identified such an exemption and to show how the professional secrecy obligation directly addresses the data controller such that it prohibits the data controller from providing all of the information set out in Articles 14.1, 14.2 and 14.4 to the data subject.

第14條第5項第d款規定，當個人資料「*依據歐盟或成員國法律所定專業保密義務之規範(包括法定之保密義務)，應予保密*」時，可免除對資料控管者提供資訊之要求。若資料控管者欲援用此例外規定，必須能夠證明其已適當確認此類例外，且說明專業保密義務如何直接規範資料控管者，以禁止資料控管者向當事人提供所有第14條第1項、第2項和第4項規定之資訊。

Example

示例

A medical practitioner (data controller) is under a professional obligation of secrecy in relation to his patients' medical information. A patient (in respect of whom the obligation of professional secrecy applies) provides the medical practitioner with information about her health relating to a genetic condition, which a number of her close relatives also have. The patient also provides the medical practitioner with certain personal data of her relatives (data subjects) who have the same condition. The medical practitioner is not required to provide those relatives with Article 14 information as the exemption in Article 14.5(D) applies. If the medical practitioner were to provide the Article 14 information to the relatives, the obligation of professional secrecy, which he owes to his patient, would be violated.

醫生（資料控管者）對其病患的醫療資訊負有專業保密義務。病患（適用於專業保密義務者）向醫生提供有關其遺傳情況的健康資訊，該遺傳情況亦發生在病患的某些近親身上。病患還向醫生提供具有相同症狀親屬（當事人）的某些個人資料。基於第14條第5項第d款之豁免，醫生無需向這些親屬提供第14條之資訊。若醫生向親屬提供第14條之資訊，則違反其對病患之專業保密義務。

Restrictions on data subject rights

當事人權利之限制

68. Article 23 provides for Member States (or the EU) to legislate for further restrictions on the scope of the data subject rights in relation to transparency and the substantive data subject rights[55] where such measures respect the essence of the fundamental rights and freedoms and are necessary and proportionate to safeguard one or more of the ten objectives set out in Article 23.1(A) to (j). Where such national measures lessen either the specific data subject rights or the general transparency obligations, which would otherwise apply to data controllers under the GDPR, the data controller should be able to demonstrate how the national provision applies to them. As set out in Article 23.2(h), the legislative measure must contain a provision as to the right of the data subject to be informed about a restriction on their rights, unless so informing them may be prejudicial to the purpose of the restriction. Consistent with this, and in line with principle of fairness, the data controller should also inform data subjects that they are relying on (or will rely on, in the event of a particular data subject right being exercised) such *a national legislative restriction* to the exercise of data subject

rights, or to the transparency obligation, unless doing so would be prejudicial to the purpose of the legislative restriction. As such, transparency requires data controllers to provide adequate upfront information to data subjects about their rights and any particular caveats to those rights which the controller may seek to rely on, so that the data subject is not taken by surprise at a purported restriction of a particular right when they later attempt to exercise it against the controller. In relation to pseudonymisation and data minimisation, and insofar as data controllers may purport to rely on Article 11 of the GDPR, WP29 has previously confirmed in Opinion 3/ 2017[56] that Article 11 of the GDPR should be interpreted as a way of enforcing genuine data minimisation without hindering the exercise of data subject rights, and that the exercise of data subject rights must be made possible with the help of additional information provided by the data subject.

第23條規定成員國（或歐盟）得在尊重基本權利和自由之本質，並為保障第23條第1項第a至j款10項目的中之一項或多項之必要且符合比例原則時，就與當事人權利範圍相關之透明化和實質當事人權利[55]為進一步限制。若此類國家措施減少特定當事人權利，或依GDPR應適用於資料控管者之一般透明化義務時，資料控管者應能夠證明國家法規如何適用。如第23條第2項第h款所述，除非有損害限制目的之虞，否則立法措施必須包含當事人有權被告知其權利受到限制之規定。同樣地，基於公正原則，除非有損立法限制目的之虞，否則資料控管者亦應告知當事人行使權利或透明化義務之限制所依據（或在當事人行使特定權利時將依據）之*國家法律為何*。因此，透明化要求資料控管者向當事人提供與其權利相關之所有資訊，以及控管者對該權利得以採行之任何特別中止情事，使當事人嗣後試圖對控管者行使其特定權利時，不至因可能之限制而感到意外。就假名化和資料最小化，以及資料控管者可能援用之GDPR第11條而言，WP29先前已在第3/2017[56]號意見中確認，GDPR第11條應被解釋為在不妨礙當事人權利行使之情況下，執行實質資料最小化的一種方式，且必須藉由當事人提供其他資訊以實現當事人權利之行使。

69. Additionally, Article 85 requires Member States, by law, to reconcile data protection with the right to freedom of expression and information. This requires, amongst other things, that Member States provide for appropriate exemptions or derogations from certain provisions of the GDPR (including from the transparency requirements under Articles 12 - 14) for processing carried out for journalistic, academic, artistic or literary expression purposes, if they are necessary to reconcile the two rights.

---

[55] As set out in Articles 12 to 22 and 34, and in Article 5 insofar as its provisions correspond to the rights and obligations provided for in Articles 12 to 22.
如第12條至第22條和第34條以及第5條所述，該條款須與第12條至第22條規定之權利和義務相對應。

[56] Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) – see paragraph 4.2
第03/2017號意見關於在合作智能運輸系統（C-ITS）之個人資料運用 - 請參閱第4.2段。

此外，第85條要求成員國依法調和資料保護與言論及資訊自由權，除其他事項外，成員國因新聞、學術、藝術或文學言論目的之運用，而有必要調和此二項權利時，得就GDPR某些條款之適用予以適當的豁免或免除（包括第12-14條之透明化要求）。

Transparency and data breaches

透明化和個資侵害

70. WP29 has produced separate Guidelines on Data Breaches[57] but for the purposes of these guidelines, a data controller's obligations in relation to communication of data breaches to a data subject must take full account of the transparency requirements set out in Article 12.[58] The communication of a data breach must satisfy the same requirements, detailed above (in particular for the use of clear and plain language), that apply to any other communication with a data subject in relation to their rights or in connection with conveying information under Articles 13 and 14.

WP29另制定了個資侵害指引[57]，但就本指引而言，資料控管者關於與當事人就個資侵害進行溝通之義務，必須充分考量第12條[58]規定之透明化要求。就個資侵害之溝通必須符合前文所述之相同要件（尤其是使用明確和簡明之語言），這些要件於與當事人就其權利或就第13條和第14條所須提供之資訊進行溝通時亦適用之。

[57] Guidelines on Personal data breach notification under Regulation 2016/679, WP 250
WP250，關於第2016/679號規則(GDPR)中的個人資料侵害通知之指引。

[58] This is made clear by Article 12.1 which specifically refers to "…any communication under Articles 15 to 22 **and 34** relating to processing to the data subject..." [emphasis added].
第12條第1項明確規定並具體提及「...依據第15條至第22條**和第34條**所定關於對當事人所為運用之任何溝通...」[重點強調]。

Annex

Information that must be provided to a data subject under Article 13 or Article 14

Required Information Type	Relevant article (if personal data collected directly from data subject)	Relevant article (if personal data not collected directly from data subject)	WP29 comments on information requirement
The identity and contact details of the controller and where application, their representatives[59]	Article 13.1(a)	Article 14.1(a)	This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address, etc)
Contact details for the data protection officer, where applicable	Article 13.1(b)	Article 14.1(b)	See WP29 Guidelines on Data Protection Officers[60]
The purposes and legal basis for the processing	Article 13.1(c)	Article 14.1(c)	In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 must be specified. In the case of special categories of personal data, the relevant provision of Article 9 (and where relevant, the applicable Union or Member State law under which the data is processed) should be specified. Where, pursuant to Article 10, personal data relating to criminal convictions and offences or related security measures based on Article 6.1 is processed, where applicable the relevant Union or Member State law under which the processing is carried out should be specified.
Where legitimate interests (Article 6.1(F)) is the legal basis for the processing, the legitimate interests pursued by the data controllers or third party	Article 13.1(d)	Article 14.2(b)	The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the controller can also provide the data subject with the information from the balancing test, which must be carried out to allow reliance on Article 6.1(F) as a lawful basis for processing, in

			advance of any collection of data subject's personal data. To avoid information fatigue, this can be included within a layered privacy statement /notice (see paragraph 35). In any case, the WP29 position is that information to the data subject should make it clear that they can obtain information on the balancing test upon request. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly or they wish to file a complaint with a supervisory authority.
Categories of personal data concerned	Not required	Article 14.1(d)	This information is required in an Article 14 scenario because the personal data has not been obtained from the data subject, who therefore lacks an awareness of which categories of their personal data the data controller has obtained.
Recipients[61] (or categories of recipients) of the personal data	Article 13.1(e)	Article 14.1(e)	The term "recipient" is defined in Article 4.9 as *"a natural or legal person, public authority, agency or another body, to which the personal data are disclosed,* ***whether a third party or not****" [emphasis added].* As such, a recipient does not have to be a third party. Therefore, other data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term "recipient" and information on such recipients should be provided in addition to information on third party recipients. The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will

			generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.
Details of transfers to third countries, the fact of same and the details of the relevant safeguards[62] (including the existence or absence of a Commission adequacy decision[63]) and the means to obtain a copy of them or where they have been made available	Article 13.1(f)	Article 14.1(f)	The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article 45/binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.
The storage period (or if not possible, criteria used to determine that period)	Article 13.2(A)	Article 14.2(a)	This is linked to the data minimization requirement in Article 5.1(C) and storage limitation requirement in Article 5.1(E). The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for

			the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purpose, including where appropriate, archiving periods.
The rights of the data subject to: • access; • rectification; • erasure; • restriction on processing; • objection to processing and • portability.	Article 13.2(B)	Article 14.2(c)	This information should be specific to the processing scenario and include a summary of what the right involves and how the data subject can take steps to exercise it any limitations on the right (see paragraph 68 above). In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information.[64] In relation to the right to portability, see WP29 Guidelines on the right to data portability.[65]
Where processing is based on consent (or explicit consent), the right to withdraw consent at any time	Article 13.2(C)	Article 14.2(d)	This information should include how consent may be withdrawn, taking into account that it should be as easy for a data subject to withdraw consent as to give it.[66]
The right to lodge a complaint with a supervisory authority	Article 13.2(D)	Article 14.2(e)	This information should explain that, in accordance with Article 77, a data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or of an alleged infringement of the GDPR.
Whether there is a statutory or contractual requirement to provide the information or whether it is necessary to enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure.	Article 13.2(E)	Not required	For example in an employment context, it may be a contractual requirement to provide certain information to a current or prospective employer. Online forms should clearly identify which fields are "required", which are not, and what will be the consequences of not filling in the

			required fields.
The source from which the personal data originate, and if applicable, whether it came from a publicly accessible source	Not required	Article 14.2(f)	The specific source of the data should be provided unless it is not possible to do so – see further guidance at paragraph 60. If the specific source is not named then information provided should include: the nature of the sources (i.e. publicly/ privately held sources) and the types of organisation/ industry/ sector.
The existence of automated decision-making including profiling and, if applicable, meaningful information about the logic used and the significance and envisaged consequences of such processing for the fata subject	Article 13.2(F)	Article 14.2(g)	See WP29 Guidelines on automated individual decision -making and Profiling.[67]

附錄

依據第13條或第14條必須提供予當事人之資訊

所需資訊類型	相關條款（若直接從當事人蒐集個人資料）	相關條款（若並非直接從當事人蒐集個人資料）	WP29對資訊要求之意見
控管者之身分和聯絡方式，及其代表[59]（如適用）	第13條第1項第a款	第14條第1項第a款	此類資訊應可輕易辨別控管者，且可與資料控管者進行不同形式之溝通（例如電話號碼，電子郵件，郵政地址等）。
個資保護長之聯絡方式（如適用）	第13條第1項第b款	第14條第1項第b款	請參閱WP29個資保護長指引[60]
運用目的和法律依據	第13條第1項第c款	第14條第1項第c款	除表明運用個人資料之目的外，依第6條規定之相關法律依據亦須具體指明。對於特種個人資料，應當具體指明第9條之相關規定（及運用該資料應適用之相關歐盟或成員國法律）。依據第10條，涉及刑事前科與犯罪或第6條第1項相關安全措施之個人資料運用，若適用相關歐盟或成員國法律，亦應具體指明。
當運用之法律依據為資料控管者或第三人追求之合法利益（第6條第1項第f款）	第13條第1項第d款	第14條第2項第b款	為確保當事人之權益，必須說明具體相關利益。於蒐集任何當事人之個人資料前，必須依據第6條第1項F款辦理平衡判斷，作為運用之合法依據，而作為最佳實務，控管者亦可向當事人提供平衡判斷之資訊。

[59] As defined by Article 4.17 of the GDPR (and referenced in Recital 80), "representative" means natural or legal person established in the EU who is designated by the controller or processor in writing under Article 27 and represents the controller or processor with regard to their respective obligations under the GDPR. This obligation applies where, in accordance with Article 3.2, the controller or processor is not established in the WU but processes the personal data of data subjects who are in the EU, and the processing relates to the offer of goods or services to, or monitoring of the behavior of, data subjects in the EU.
依據GDPR第4條第17款（並參考前言第80點）中之定義，「代表」係指設立於歐盟境內之自然人或法人，由控管者或受託運用者依據第27條以書面形式指定，並代表控管者或受託運用者履行GDPR下各自之義務。依據第3條第2項，該義務適用於當控管者或受託運用者非設立於歐盟境內，但運用位於歐盟境內當事人之個人資料，且該運用涉及對歐盟境內當事人提供商品或服務或監控其行為。

[60] Guidelines on Data Protection Officers, WP243 rev.01, last revised and adopted on 5 April 2017.
WP243 rev.01，個資保護長指引，於2017年4月5日最終修訂並通過。

			為避免資訊疲勞，可將其包含在分層隱私聲明/通知中（請參閱第35段）。無論如何，WP29之立場為，提供予當事人之資訊應明確表明可依據要求取得有關平衡判斷之資訊。這對於有效之透明化極為重要，尤其是當事人對平衡判斷之測試執行是否公正有疑慮，或希望向監管機關提請申訴時。
相關個人資料類型	無相關規定	第14條第1項第d款	第14條要求提供此類資訊，由於個人資料並非從當事人取得，因此當事人無法知悉資料控管者取得何種類型之個人資料。
個人資料接收者[61]（或接收者類型）	第13條第1項第e款	第14條第1項第e款	第4條第9款將「接收者」一詞定義為「*向其揭露個人資料之自然人或法人、公務機關、局處或其他機構，**不論其是否為第三方***」[*重點強調*]。所以，接收者不需為第三方。因此，「接收者」一詞涵蓋了向其傳送或揭露資料之其他資料控管者、共同控管者和受託運用者。且除了有關第三方接收者之資訊外，亦應提供有關此類接收者之資訊。 必須提供個人資料實際（指明）接收者或接收者之類型。基於公正原則，控管者必須提供對當事人最有意義的接收者資訊。實際上，此通常為指名接收者，以便當事人確切知道誰擁有其個人資料。若控管者選擇提供接收者類型，則資訊亦應透過表明接收者之類型（即參考其執行之活動）、行業、部門和子部門以及接收者的所在位置等方式，盡可能具體指明。
移轉至第三國之詳細資訊、相同維護措施之事實及	第13條第1項第f款	第14條第1項第f款	GDPR相關條文規定需具體表明資料之移轉和對應機制（例如，第45條的適足性認定/ 第47條的有拘束力之企業守則/ 第46

[61] As defined by Article 4.9 of the GDPR and referenced in Recital 31
依GDPR第4條第9款定義，並參考前言第31點。

相關維護措施之詳細資訊（包括執委會是否做出適足性之決定[63]）、以及取得這些維護措施副本之方式或可於何處取得			第2項的標準資料保護條款，第49條的例外和安全維護措施等）。亦應提供造訪或取得相關文件地點和方式之資訊，例如：透過提供所用機制之網址連結。基於公正原則，向第三國移轉資訊之提供應盡可能對當事人是有意義的；此通常意味著指明第三國國家。
儲存期限（若不可行，則為決定該期限之標準）	第13條第2項第a款	第14條第2項第a款	此與第5條第1項第c款中資料最少化要求和第5條第1項第e款中儲存限制要求相關。儲存期限（或決定期限之標準）可能由法定要求或行業指引等因素決定，但應允許當事人依據其自身情況評估對特定資料/目的之保留期限為何。若資料控管者的一般聲明為只要就運用之合法目的為必要，資料將盡可能長時間的被保留，則該聲明是不足夠的。在相關情況下，應針對不同類型之個人資料和/或不同運用目的規定不同之儲存期限。（包括適當歸檔期限）
當事人基於其權利得： • 近用 • 改正 • 刪除 • 限制運用 • 拒絕運用 • 可攜	第13條第2項第b款	第14條第2項第c款	此資訊應特定於運用情景，並提供概括資訊，包含所涉及之權利、當事人行使其權利之步驟以及對該權利之任何限制（請參閱前文第68段）。 尤其是，最遲在與當事人進行第一次溝通時，必須明確地使當事人注意到其拒絕運用之權利，且必須與任何其他資訊清楚地分開提供。[64] 關於可攜性，請參閱WP29資料可攜權之指引。[65]

[62] As set out in Article 46.2 and 46.3
如第46條第2項和46條第3項所述。
[63] In accordance with Article 45
依據第45條。
[64] Article 21.4 and Recital 70 (which applies in the case of direct marketing)
第21條第4項和前言第70點（適用於行銷案例）。
[65] Guidelines on the right to data portability, WP 242 rev.01, last revised and adopted on 5 April 2017
WP 242 rev.01，資料可攜權指引，於2017年4月5日最終修訂並通過。

基於同意（或明確同意）所為之運用，有權隨時撤回同意	第13條第2項第c款	第14條第2項第d款	此資訊應包含如何撤回同意，同時考量到撤回同意應和給予同意一樣容易。[66]
向監管機關提出申訴之權利	第13條第2項第d款	第14條第2項第e款	此資訊應說明，依據第77條，當事人有權向監管機關提出申訴，特別是在其慣常居住地、工作地點或被指控違反GDPR之地點。
是否有法定或契約要求提供資訊，或是否有必要簽訂契約，或者是否有義務提供資訊以及未提供資訊可能之後果	第13條第2項第e款	無相關規定	例如，在工作環境中，契約可能要求提供某些資訊予目前或未來雇主。 網路表格應清楚表明哪些資訊是「必需的」，哪些不是，以及未填寫必填資訊之後果。
個人資料原始來源，如適用，是否來自可公開造訪之來源	無相關規定	第14條第2項第f款	除非無可能性，否則應提供具體資料來源—進一步指導請參閱第60段。若無法指名特定來源，則提供之資訊應包括：資料來源之性質（即公開/私人來源）和組織/行業/部門之類型。
自動化決策之存在，包括剖析和（如適用）與運用邏輯相關之有意義的資訊以及此類運用對當事人之重要性和預設之後果。	第13條第2項第f款	第14條第2項第g款	請參閱WP29關於自動化個人決策和剖析指引。[67]

[66] Article 7.3
第7條第3項。
[67] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251
WP 251，關於第2016/679號規則(GDPR)中的自動化個人決策和剖析之指引。