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

17/EN
WP259rev.01

# Article29 Working Party
# 第29條個資保護工作小組

# Guidelines on consent under Regulation 2016/679
# 關於第2016/679號規則(GDPR)中的同意之指引

**Adopted on 28 November 2017**
**As last Revised and Adopted on 10 April 2018**
**2017年11月28日通過**
**2018年4月10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/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

# Contents 目錄

1. Introduction 導言 ..... 3
2. Consent in Article 4(11) of the GDPR GDPR 第 4 條第 11 款規定之同意 ..... 5
3. Elements of valid consent 有效同意的要素 ..... 6
3.1. Free / freely given 自主性/自主給予 ..... 6
3.1.1. Imbalance of power 權力不對等 ..... 7
3.1.2. Conditionality 條件性 ..... 10
3.1.3. Granularity 區別性 ..... 13
3.1.4. Detriment 損害 ..... 14
3.2. Specific 特定性 ..... 16
3.3. Informed 知情性 ..... 18
3.3.1. Minimum content requirements for consent to be 'informed' 知情同意之內容的最低要求 ..... 18
3.3.2. How to provide information 提供資訊的方式 ..... 19
3.4. Unambiguous indication of wishes 非模糊的意思表示 ..... 22
4. Obtaining explicit consent 獲得明確同意 ..... 26
5. Additional conditions for obtaining valid consent 獲得有效同意的其他條件 ..... 29
5.1. Demonstrate consent 證明同意 ..... 29
5.2. Withdrawal of consent 撤回同意 ..... 31
6. Interaction between consent and other lawful grounds in Article 6 GDPR 同意與 GDPR 第 6 條其他合法基礎的適用關係 ..... 33
7. Specific areas of concern in the GDPR GDPR 中的特定領域考量 ..... 34
7.1. Children (Article 8) 兒童（第 8 條） ..... 34
7.1.1. Information society service 資訊社會服務 ..... 35
7.1.2. Offered directly to a child 直接對兒童提供 ..... 36
7.1.3. Age 年齡 ..... 36
7.1.4. Children's consent and parental responsibility 兒童同意與法定代理權 ..... 38
7.2. Scientific research 科學研究 ..... 40
7.3. Data subject's rights 當事人權利 ..... 44
8. Consent obtained under Directive 95/46/EC 在 95/46/EC 指令下獲得之同意 ..... 44

## 1. Introduction
## 導言

These Guidelines provide a thorough analysis of the notion of consent in Regulation 2016/679, the General Data Protection Regulation (hereafter: GDPR). The concept of consent as used in the Data Protection Directive (hereafter: Directive 95/46/EC) and in the e-Privacy Directive to date, has evolved. The GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. These Guidelines focus on these changes, providing practical guidance to ensure compliance with the GDPR and building upon Opinion 15/2011on consent. The obligation is on controllers to innovate to find new solutions that operate within the parameters of the law and better support the protection of personal data and the interests of data subjects.

本指引對2016/679規則，即一般資料保護規則（以下稱為GDPR）中的同意之概念提供詳盡的分析。在資料保護指令（以下稱為95/46/EC指令）與電子隱私指令中使用迄今的同意之觀念已有所演進。GDPR對於獲得及舉證有效同意之規範，提出進一步的澄清與詳細說明。本指引聚焦於這些變動，提出實務指引以確保GDPR的遵循性，並以15/2011關於同意之意見為基礎。控管者有義務創新找尋新的解決方案以在法律界限內運作，並更佳得維持個人資料與當事人利益之保護。

Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR.[1] When initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing.
如GDPR第6條所列舉[1]，同意仍為運用（譯註：我國個資法將個資之使用分為蒐集(collection)、處理 (processing)、利用 (use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本譯文因此將GDPR中的processing譯為「運用」，而 processor 譯為「受託運用者」）個人資料的六種合法基礎之一。當啟動涉及運用個人資料之行動時，控管者必須花些時間考量何者對該設想的運用是最適當的合法根據。

Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.[2]
一般來說，同意只有在當事人取得控制權，且對於接受或拒絕條件，或拒絕條件而免受損害享有真正的選擇時，才可作為適當的合法基礎。在尋求同意時，控管者有責任評估是否符合獲得有效同意的所有規範。如完全遵守GDPR而獲得，同意即為賦予當事人對與其有關之個

[1] Article 9 GDPR provides a list of possible exemptions to the ban on processing special categories of data. One of the exemptions listed is the situation where the data subject provides explicit consent to the use of this data.
GDPR第9條對特種個資的運用禁止提供數項可適用的例外。其中之一即是當事人明確同意使用該資料。

[2] See also Opinion 15/2011 on the definition of consent (WP 187), pp. 6-8, and/or Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 9, 10, 13 and 14.
見15/2011關於同意的定義之意見書（WP187），第6頁至第8頁，及/或06/2014關於95/46/EC指令第7條下的資料控管者之正當利益的概念之意見書（WP217），第9頁、第10頁、第13頁及第14頁。

人資料可否被運用之控制權的工具。若否，則當事人的控制權形同虛設，而同意將成為無效的運用依據，並導致運用行為違法[2]。

The existing Article 29 Working Party (WP29) Opinions on consent[3] remain relevant, where consistent with the new legal framework, as the GDPR codifies existing WP29 guidance and general good practice and most of the key elements of consent remain the same under the GDPR. Therefore, in this document, WP29 expands upon and completes earlier Opinions on specific topics that include reference to consent under Directive 95/46/EC, rather than replacing them.
現有的第29條工作小組（WP29）關於同意的意見[3]仍然具有相關性，這與新的法律框架一致，因為GDPR納入了現有的WP29指引和一般優良實務，並且GDPR下的大多數有關同意的關鍵要素保持不變。因此，在本文件中，WP29擴充並完備了早期關於特定主題的意見，其中也包括95/46/EC指令下的同意，而不是替換它們。

As stated in Opinion 15/2011 on the definition on consent, inviting people to accept a data processing operation should be subject to rigorous requirements, since it concerns the fundamental rights of data subjects and the controller wishes to engage in a processing operation that would be unlawful without the data subject's consent.[4] The crucial role of consent is underlined by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Furthermore, obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this would not legitimise collection of data which is not necessary in relation to a specified purpose of processing and be fundamentally unfair.[5]
正如意見15/2011中關於同意的定義所述，要求他人接受的資料運用作業應該受到嚴格規範，因為它涉及當事人的基本權利，並且若未經當事人同意，控管者對資料的運用作業即為非法[4]。「歐盟基本權利憲章」第7條和第8條強調了同意的重要性。此外，獲得同意並非否定或以任何方式限縮控管者遵守GDPR中有關資料運用原則的義務，尤其是GDPR第5條關於公平性、必要性、比例性以及資料品質的義務。即便運用個資是基於當事人的同意，但與特定資料運用目的無必要的資料蒐集，既不合法，基本上也不公平[5]。

Meanwhile, WP29 is aware of the review of the ePrivacy Directive (2002/58/EC). The notion of consent in the draft ePrivacy Regulation remains linked to the notion of consent in the GDPR.[6] Organisations are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software. WP29 has already provided recommendations and guidance to the European legislator on the Proposal for a Regulation on ePrivacy.[7]
同時，WP29也意識到對電子隱私指令（2002/58/EC）的審查。電子隱私規則草案中的同意

[3] Most notably, Opinion 15/2011 on the definition of consent (WP 187).
尤其是15/2011關於同意的定義之意見書（WP187）。
[4] Opinion 15/2011, page on the definition of consent (WP 187), p.8
15/2011關於同意的定義之意見書（WP187），第8頁。
[5] See also Opinion 15/2011 on the definition of consent (WP 187), and Article 5 GDPR.
見15/2011關於同意的定義之意見書（WP187），以及GDPR第5條。
[6] According to Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Articles 4(11) and Article 7 of the GDPR apply.
依電子隱私規則草案第9條規定，該規則適用GDPR第4條第11款及第7條關於同意的定義與要件。
[7] See Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (WP 240).
見03/2016關於電子隱私指令的評估與審查之意見書（WP240）。

之概念仍準用GDPR中的同意之概念[6]。組織在電子隱私法規下，對於大部分的線上行銷訊息或行銷電話，以及包含使用cookies或行動應用程式或其他軟體在內的線上追蹤手段，可能都需要獲得同意。WP29已向歐洲立法機關就電子隱私規則之草案提出建議與指引[7]。

With regard to the existing e-Privacy Directive, WP29 notes that references to the repealed Directive 95/46/EC shall be construed as references to the GDPR.[8] This also applies to references to consent in the current Directive 2002/58/EC, as the ePrivacy Regulation will not (yet) be in force from 25 May 2018. According to Article 95 GDPR, additional obligations in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks shall not be imposed insofar the e-Privacy Directive imposes specific obligations with the same objective. WP29 notes that the requirements for consent under the GDPR are not considered to be an 'additional obligation', but rather as preconditions for lawful processing. Therefore, the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive.

對於現有的電子隱私指令，WP29指出原本應參照已廢止的95/46/EC指令之處，應解釋為參照GDPR[8]。此亦適用於現行2002/58/EC指令中的同意之參照，因為電子隱私規則在2018年5月25日時（尚）不會生效。依GDPR第95條規定，在電子隱私指令就「以大眾通訊網路提供大眾電子通訊服務」所涉及的運用已課予特定義務之範圍內，GDPR即不再對相同目標課以額外義務。WP29指出，GDPR下的同意之規範並不構成「額外義務」，反而是合法運用的先決條件。因此，GDPR關於獲得有效同意之條件，對於落入電子隱私指令範圍之情形即有適用。

### 2. Consent in Article 4(11) of the GDPR<br>GDPR第4條第11款規定之同意

Article 4(11) of the GDPR defines consent as: *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*

GDPR第4條第11款將同意定義為：「*當事人為表達同意運用與其有關之個人資料，藉由聲明或清楚肯定之行動而自由給予之特定、知情及非模糊之意思表示*」。

The basic concept of consent remains similar to that under the Directive 95/46/EC and consent is one of the lawful grounds on which personal data processing has to be based, pursuant to Article 6 of the GDPR.[9] Besides the amended definition in Article 4(11), the GDPR provides additional

[8] See Article 94 GDPR.
見GDPR第94條。

[9] Consent was defined in Directive 95/46/EC as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" which must be 'unambiguously given' in order to make the processing of personal data legitimate (Article 7(a) of Directive 95/46/EC)). See WP29 Opinion 15/2011 on the definition of consent (WP 187) for examples on the appropriateness of consent as lawful basis. In this Opinion, WP29 has provided guidance to distinguish where consent is an appropriate lawful basis from those where relying on the legitimate interest ground (perhaps with an opportunity to opt out) is sufficient or a contractual relation would be recommended. See also WP29 Opinion 06/2014, paragraph III.1.2, p. 14 and further. Explicit consent is also one of the exemptions to the prohibition on the processing of special categories of data: See Article 9 GDPR.
95/46/EC指令對同意的定義為「當事人為表達同意運用與其有關之個人資料所自由給予之特定且知情的意思表示」，且須「非模糊地給予」才可使該個資運用行為合法（95/46/EC指令第7條第a項）。見15/2011關於同意的定義之意見書（WP187）中有關以同意作為合法基礎的適當性的範例。在該意見書中，WP29對於如何區別「以同意作為適當的合法基礎」以及「以充足正當利益作為合法基礎（或許伴隨選擇退出的機會）」或「建議採用契約關係作為合法基礎」提出指引。見第29條工作組06/2014意見書，第14頁，第III.1.2段以下。明確同意同時也是禁止運用特種個資的一項例外：見GDPR第9條。

guidance in Article 7 and in recitals 32, 33, 42, and 43 as to how the controller must act to comply with the main elements of the consent requirement.
同意的基本觀念仍與95/46/EC指令中基本觀念的相似，且依GDPR第6條規定[9]，同意是個人資料運用所須依據的合法基礎之一。除了第4條第11款修正的定義之外，GDPR於第7條及前言第32點、第33點、第42點與第43點，就控管者須如何行動以遵循同意之規範的重要要素提出額外指引。

Finally, the inclusion of specific provisions and recitals on the withdrawal of consent confirms that consent should be a reversible decision and that there remains a degree of control on the side of the data subject.
最後，條文中包含撤回同意的具體條款及前言，即確認同意應為可逆的決定，當事人一方仍有一定程度的控制權。

## 3. Elements of valid consent
## 有效同意的要素

Article 4(11) of the GDPR stipulates that consent of the data subject means any:
GDPR第4條第11款規定當事人的同意係指任何：

- freely given,
  自主給予
- specific,
  特定
- informed and
  知情以及
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
  非模糊的當事人意思表示，即藉由聲明或清楚肯定之行動，表達同意運用與其有關之個人資料。

In the sections below, it is analysed to what extent the wording of Article 4(11) requires controllers to change their consent requests/forms, in order to ensure compliance with the GDPR. [10]以下章節將分析第4條第11款規範控管者改變其同意之要求／形式的文義範圍，以確保GDPR的遵循性[10]。

### 3.1. Free / freely given[11]

[10] For guidance with regard to ongoing processing activities based on consent in Directive 95/46, see chapter 7 of this document and recital 171 of the GDPR.
關於依據95/46/EC指令的同意規範而進行的運用活動，其指引詳見本文件第7章及GDPR前言第171點。

[11] In several opinions, the Article 29 Working Party has explored the limits of consent in situations where it cannot be freely given. This was notably the case in its Opinion 15/2011 on the definition of consent (WP 187), Working Document on the processing of personal data relating to health in electronic health records (WP 131), Opinion 8/2001 on the processing of personal data in the employment context (WP48), and Second opinion 4/2009 on processing of data by the World Anti-Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations (WP 162).
WP29在幾份意見書中探討在無法自主給予同意的情形將使同意受到的限制。特別是15/2011關於同意的定義之意見書（WP187）、關於運用與電子健康紀錄有關健康資訊的個人資料之工作文件（WP131）、8/2001關於雇傭關係中的個人資料運用之意見書（WP48），以及4/2009關於世界運動禁藥管制組織（WADA）隱私與個人資訊保護國際標準、世界運動禁藥管制規範相關條文，以及WADA與（國家）反禁藥組織對抗運動禁藥中的隱私議題所涉個資運用行為之第二份意見書（WP162）。

**自主性/自主給予**[11]

The element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.[12] If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.[13] The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR.

「自主」要素意指當事人真正的選擇與控制權。作為一部通用規則，GDPR規定若當事人未能獲得真正的選擇，或受到強迫而作出同意，或如不同意將使其遭受負面後果時，該同意即為無效[12]。如將同意綑綁於條款與條件中，成為無法磋商的一部分時，即推定為非自主給予。因此，若當事人無法拒絕或撤回同意而免受任何損害時，其同意即不被認為具備自主性[13]。GDPR亦將控管者與當事人間的不對等之概念納入考量。

When assessing whether consent is freely given, one should also take into account the specific situation of tying consent into contracts or the provision of a service as described in Article 7(4). Article 7(4) has been drafted in a non-exhaustive fashion by the words "inter alia", meaning that there may be a range of other situations which are caught by this provision. In general terms, any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.

在評估同意是否自主給予時，也應考量第7條第4項所描述將同意與契約或提供之服務綑綁的情形。第7條第4項使用「特別是」(inter alia)一詞以例示方式草擬該條款，即表示得有其他情形落入本條款規範。大體而言，任何對當事人造成不適當之壓力或影響而使當事人無法行使自由意願的要素（可能以許多不同方式顯現），均應導致同意無效。

[Example 1]
A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geo-localisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

[示例1]
某相片編輯行動應用程式向使用者要求啟用衛星定位功能以使用其服務。此應用程式亦告知使用者將基於行為廣告之目的而利用所蒐集的資料。無論地理位置或線上行為廣告皆非相片編輯服務所必要，且逾越提供其核心服務之範圍。鑒於使用者若不同意該目的即無法使用此應用程式，其同意即無法認定為自主給予。

### 3.1.1. Imbalance of power
### 權力不對等

Recital 43[14] clearly indicates that it is unlikely that **public authorities** can rely on consent for

[12] See Opinion 15/2011 on the definition of consent (WP187), p. 12
見15/2011關於同意的定義之意見書（WP187），第12頁。

[13] See Recitals 42, 43 GDPR and WP29 Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, (WP 187), p. 12.
見GDPR前言第42點、第43點及WP29於2011年7月13日通過的15/2011關於同意的定義之意見書（WP187），第12頁。

[14] Recital 43 GDPR states: "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular

processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. WP29 considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.[15]

前言第43點[14]清楚指出，**公務機關**不太可能以同意作為運用個資的依據，因為當公務機關作為一個控管者時，其與當事人之間經常有明顯的權力不對等情形。在大部分案例也明顯存在當事人對於是否接受控管者運用個資（的條件）並無真正的選擇權利之情況。WP29認為，在原則上，應有其他合法基礎更適合作為公務機關行為之依據[15]。

Without prejudice to these general considerations, the use of consent as a lawful basis for data processing by public authorities is not totally excluded under the legal framework of the GDPR. The following examples show that the use of consent can be appropriate under certain circumstances.

在不牴觸上述總體考量的前提下，GDPR的法律框架並不完全排除公務機關以同意作為運用個資的合法基礎。下列示例即說明某些可適當使用同意的情形。

> [Example 2] A local municipality is planning road maintenance works. As the road works may disrupt traffic for a long time, the municipality offers its citizens the opportunity to subscribe to an email list to receive updates on the progress of the works and on expected delays. The municipality makes clear that there is no obligation to participate and asks for consent to use email addresses for this (exclusive) purpose. Citizens that do not consent will not miss out on any core service of the municipality or the exercise of any right, so they are able to give or refuse their consent to this use of data freely. All information on the road works will also be available on the municipality's website.
>
> [示例2]某地方政府正在規劃道路養護工程。由於該道路工程可能長時間妨礙交通，該政府提供其市民以電子郵件訂閱工程進度及預期延工等資訊的機會。該政府清楚告知市民並無參與義務，並基於該（單一）目的徵求使用電子郵件地址之同意。不同意的市民不會因此無法獲得該政府的核心服務或無法行使任何權利，因此市民得自主地對該利用行為表示同意或拒絕。該道路工程的所有資訊亦皆可於政府網站上取得。

> [Example 3] An individual who owns land needs certain permits from both her local municipality and from the provincial government under which the municipality resides. Both public bodies require the same information for issuing their permit, but are not accessing each other's databases. Therefore, both ask for the same information and the land owner sends out her details to both public bodies. The municipality and the provincial authority ask for her consent to merge the files, to avoid duplicate procedures and correspondence. Both public bodies ensure that this is optional and that the permit requests will still be processed separately if she decides not to consent to the merger of her data. The land owner is able to give consent to the authorities for the purpose of merging the files freely.
>
> [示例3]某自然人擁有之土地需取得地方政府及該地方政府所在地之省政府的特定許可。兩公務機關為發布許可，需取得相同之資訊，但卻無法存取彼此的資料庫。因此，雙方皆要求提供相同之資訊，而該土地所有人即將資料寄送予兩公務機關。地方政府及省政府向該人徵求合併檔案的同意，以避免重複程序及通信聯繫等問題。兩公務機關均保證該同意具選擇性，且若該人不同意合併資料，其許可程序仍將分別進行。該土地所有人即可自主地向公務機關就合併檔案之目的給予同意。

---

where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. (…)"

GDPR前言第43點：「為確保同意為自主給予，在當事人與控管者間明顯存有不平等的特定情形，同意無法作為運用個人資料的有效法律基礎，尤其當控管者為公務機關時，在任何情況下都不太可能自主給予同意…」。

[15] See Article 6 GDPR, notably paragraphs (1c) and (1e).

見GDPR第6條，特別是第1項第c款與第1項第e款。

[Example 4] A public school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.[16]

[示例4]某公立學校徵求學生同意學校使用其照片以出版學生雜誌。只要學生不會遭拒絕提供教育或服務，並可拒絕學校使用照片而不會受到任何損害，則同意在此情形即具備真正的選擇性[16]。

An imbalance of power also occurs in the **employment** context.[17] Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.[18] Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.[19]
權力不對等的情形亦存在於**僱傭關係**中[17]。鑒於雇主與受雇人之間的從屬性，當事人不太可能可拒絕同意雇主運用其個人資料，而毋庸面臨因拒絕所致不利影響的恐懼或實際風險。舉例來說，當雇主要求同意在工作場所啟用例如攝影監視等監控機制，或要求填寫評估表格時，受雇人不太可能可自由回覆同意與否而不感到壓力[18]。因此，WP29認為雇主以同意作為運用現在或未來受雇人個資的依據仍有疑慮，因為同意不太可能是自主給予。基於雇主與受雇人間的關係，對於大部分這種運用與工作相關的個資之情形，其合法基礎不可也不應是受雇人的同意（第6條第1項第a款）[19]。

However this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.[20]
然而這並不代表雇主永遠不可以同意作為運用行為的合法基礎。在某些情況，雇主可能得證明同意為自主給予。鑒於雇主與其員工間的權力不對等，受雇人僅在例外情形，即無論同意與否均不會產生不利結果時，才能夠自主給予同意[20]。

[Example 5]

[16] For the purposes of this example, a public school means a publically funded school or any educational facility that qualifies as a public authority or body by national law.
為本示例之目的，公立學校係指公家資助的學校或任何具有國家法律認定之公務機關或團體資格的教育機構。

[17] See also Article 88 GDPR, where the need for protection of the specific interests of employees is emphasized and a possibility for derogations in Member State law is created. See also Recital 155.
見GDPR第88條強調的保護受雇人特定利益之需求，以及成員國法律可創造的例外。亦見前言第155點。

[18] See Opinion 15/2011 on the definition of consent (WP 187), pp. 12-14 , Opinion 8/2001 on the processing of personal data in the employment context (WP 48), Chapter 10, Working document on the surveillance of electronic communications in the workplace (WP 55), paragraph 4.2 and Opinion 2/2017 on data processing at work (WP 249), paragraph 6.2.
見15/2011關於同意的定義之意見書（WP187），第12頁至第14頁、8/2001關於僱傭關係中的個人資料運用之意見書（WP48）第10章、關於工作場所的電子通訊監控之工作文件（WP55），第4.2段，以及2/2017關於職業環境的資料運用（WP249），第6.2段。

[19] See Opinion 2/2017 on data processing at work, page 6-7
見2/2017關於職業環境的資料運用，第6頁至第7頁。

[20] See also Opinion 2/2017 on data processing at work (WP249), paragraph 6.2.
見2/2017關於職業環境的資料運用（WP249），第6.2段。

A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.

[示例5]

某攝影團隊將拍攝辦公室的特定區域。由於受雇人可能出現於影片的背景中，雇主即向坐在該區域內的受雇人徵求被拍攝的同意。不同意被拍攝者不會以任何方式受到處罰，而僅需在拍攝期間移至該建築內其他區域相同的辦公桌。

Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.

權力不對等不僅限於公務機關及僱傭關係，也可能存在於其他情形。如同WP29在數個意見中強調，只有在當事人可行使真正的選擇權，且若不同意亦不會有受欺瞞、脅迫、強制或重大負面結果（例如大量的額外成本）之風險時，其同意方屬有效。當存有任何強迫、壓力或無法行使自由意願的情形時，其同意絕非自主。

#### 3.1.2. Conditionality
#### 條件性

To assess whether consent is freely given, Article 7(4) GDPR plays an important role.[21]

Article 7(4) GDPR indicates that, inter alia, the situation of "bundling" consent with acceptance of terms or conditions, or "tying" the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given (recital 43). Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred.

GDPR第7條第4項對於評估同意是否自主給予扮演重要角色[21]。

GDPR第7條第4項指出，特別是將同意與接受條款或條件「綑綁」，或當運用個人資料並非某契約或服務所必要，卻將提供契約或服務與徵求運用個資之同意「綑綁」一起的情形，都是高度不樂見的。如果同意是在此情形下給予，則將被視為非自主提供（前言第43點）。第

[21] Article 7(4) GDPR: "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." See also Recital 43 GDPR, that states: "[…] Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance."
GDPR第7條第4項：「當評估同意是否自主給予時，應特別在最大程度考量包含提供服務在內的契約履行是否以同意運用履行契約非必要的個人資料為條件」。亦見GDPR前言第43點：「[…]即便在個案中尚屬適當，若不允許就不同的個人資料運用行為分別給予同意，或儘管同意對履行契約並非必要，卻使包含提供服務在內的契約履行依附於同意時，該同意將推定為非自主給予」。

7條第4項旨在確保當個人資料並非必要時，運用個資之目的不致被提供契約或服務所掩飾或與其綑綁。為了達到此目的，GDPR確保同意運用個資不可成為契約直接或間接之履行對價。同意與契約為合法運用個資的兩種合法基礎，彼此不可合併或模糊界線。

Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in the way of free consent. As data protection law is aiming at the protection of fundamental rights, an individual's control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service.
超過嚴格必要範圍而強迫同意使用個人資料，將限制當事人的選擇權，並妨礙其自主同意。由於個資保護法律之目標即在保護基本權利，因此個人對其個人資料的控制極為重要，而對於非必要個人資料之運用的同意，將強烈推定不可視為換得契約履行或服務提供的對價義務。

Hence, whenever a request for consent is tied to the performance of a contract by the controller, a data subject that does not wish to make his/her personal data available for processing by the controller runs the risk to be denied services they have requested.
因此，當控管者將徵求同意與履行契約綑綁一起時，不願意由控管者運用其個人資料之當事人即面臨遭拒絕提供其所求之服務的風險。

To assess whether such a situation of bundling or tying occurs, it is important to determine what the scope of the contract is and what data would be necessary for the performance of that contract. According to Opinion 06/2014 of WP29, the term "necessary for the performance of a contract" needs to be interpreted strictly. The processing must be necessary to fulfil the contract with each individual data subject. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to facilitate payment. In the employment context, this ground may allow, for example, the processing of salary information and bank account details so that wages can be paid.[22] There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract.
在評估是否有此類綑綁的情形時，重要的是確定該契約的範圍，以及為履行該契約所必要之個人資料。依WP29意見06/2014所述，「履行契約所必要」一語須嚴格解釋。該運用行為必須是完成個別當事人之契約所必要。例如可包含運用當事人的地址以供寄送線上購買之商品，或運用信用卡資訊以完成付款。在僱傭關係的情形，此依據可允許例如運用薪資資訊及銀行帳戶細節以支付薪酬[22]。運用資料與執行契約之目的間，必須具有直接且客觀的連結。

If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis.[23]
如控管者有意運用事實上係為履行契約所必要的個人資料，則同意即非適當的合法依據[23]。

Article 7(4) is only relevant where the requested data are **not** necessary for the performance of the

[22] For more information and examples, see Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, adopted by WP29 on 9 April 2014, p. 16-17. (WP 217).
更多資訊與示例見WP29於2014年4月9日通過之06/2014關於95/46/EC指令第7條下的資料控管者之正當利益的概念之意見書，第16頁至第17頁（WP217）。

[23] The appropriate lawful basis could then be Article 6(1)(b) (contract).
適當的合法基礎可為第6條第1項第b款（契約）。

contract, (including the provision of a service), and the performance of that contract is made conditional on the obtaining of these data on the basis of consent. Conversely, if processing **is** necessary to perform the contract (including to provide a service), then Article 7(4) does not apply.
第7條第4項僅與「要求非履行契約（包含提供服務）所必要之資料，且根據同意而獲得這些資料是履行契約的條件」相關。相反地，如運用行為是履行契約（包含提供服務）所必要，則第7條第4項即不適用。

[Example 6]
A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee, consent cannot be freely given.
[示例6]
某銀行要求客戶同意允許第三方基於行銷之目的使用其付款資訊。此運用行為對於履行與客戶間的契約及提供一般性的銀行帳戶服務並非必要。若客戶不同意該運用目的，將導致遭拒絕提供銀行服務、關閉銀行帳戶，或依案例情形增加費用時，該同意即非自主給予。

The choice of the legislator to highlight conditionality, amongst others, as a presumption of a lack of freedom to consent, demonstrates that the occurrence of conditionality must be carefully scrutinized. The term "utmost account" in Article 7(4) suggests that special caution is needed from the controller when a contract (which could include the provision of a service) has a request for consent to process personal data tied to it.
立法者選擇在各個推定同意不具自主性的要素中強調條件性，即表示如有條件的存在，則必須詳加檢視。第7條第4項中的「在最大範圍內考量」一語，即指當某契約（包含服務的提供）與要求同意運用個資綑綁一起時，控管者需特別留意。

As the wording of Article 7(4) is not construed in an absolute manner, there might be very limited space for cases where this conditionality would not render the consent invalid. However, the word "presumed" in Recital 43 clearly indicates that such cases will be highly exceptional.
由於第7條第4項的文義並非絕對，因此條件性在某些案例仍可能存有極有限的空間，不致使同意不生效力。然而，前言第43點的「推定」一詞清楚指出該類案例屬於高度例外。

In any event, the burden of proof in Article 7(4) is on the controller.[24] This specific rule reflects the general principle of accountability which runs throughout the GDPR. However, when Article 7(4) applies, it will be more difficult for the controller to prove that consent was given freely by the data subject.[25]
無論如何，控管者應就第7條第4項負舉證責任[24]。此特別規範反映了貫穿GDPR的課責性一

[24] See also Article 7(1) GDPR, which states that the controller needs to demonstrate that the data subject's agreement was freely given.
見GDPR第7條第1項，控管者須證明當事人的同意為自主給予。

[25] To some extent, the introduction of this paragraph is a codification of existing WP29 guidance. As described in Opinion 15/2011, when a data subject is in a situation of dependence on the data controller – due to the nature of the relationship or to special circumstances – there may be a strong presumption that freedom to consent is limited in such contexts (e.g. in an employment relationship or if the collection of data is performed by a public authority). With Article 7(4) in force, it will be more difficult for the controller to prove that consent was given freely by the data subject. See: Opinion 15/2011 on the definition of consent (WP 187), pp. 12-17.
某程度上，本段是現存WP29指引之彙整。如同在15/2011意見書所述，在當事人基於彼此關係的性質或特殊情況而從屬於資料控管者時，在該背景下（例如僱傭關係或由公務機關蒐集資料），可強力推定該同意之自主性受到限制。在第7條第4項的效力下，控管者較難證明同意是由當事人自主給予。見：15/2011關於同意的定義之意見書（WP187），第12頁至第17頁。

般原則。然而，當第7條第4項適用時，控管者將較難證明同意係由當事人自主給予[25]。

The controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent.
控管者得主張當事人可在「同意額外目的使用個人資料之服務」與「相同控管者所提供之等同服務，但不需同意額外目的使用個人資料」之中作出選擇，因此其組織已提供當事人真正的選擇權。只要存在使控管者履行契約或提供契約約定的服務，而不需同意其他或額外的資料使用之可能性時，即表示此處不存在有條件的服務。然而，此二種服務必須真正的實質相同。

The WP29 considers that consent cannot be considered as freely given if a controller argues that a choice exists between its service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by a different controller on the other hand. In such a case, the freedom of choice would be made dependent on what other market players do and whether an individual data subject would find the other controller's services genuinely equivalent. It would furthermore imply an obligation for controllers to monitor market developments to ensure the continued validity of consent for their data processing activities, as a competitor may alter its service at a later stage. Hence, using this argument means this consent fails to comply with the GDPR.
WP29認為，若控管者主張選擇權存在於「由該控管者提供，但須同意額外目的使用個人資料之服務」與「其他控管者提供之等同服務」之間，則該同意不可被認定為自主給予。在此情形中，選擇的自由性將依附於其他市場參與者的行為，以及個別當事人是否認為其他控管者的服務真正等同。且由於競爭者可能事後調整其服務，這表示控管者有義務監看市場發展以確保對其個資運用行為之同意持續有效。因此，提出此主張即表示該同意不符合GDPR的規範。

#### 3.1.3. Granularity
#### 區別性

A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR.
某項服務可能包含不只一種目的之數個運用行為。在此情形，當事人應可自由選擇接受何種目的，而無須一次同意所有目的。依GDPR規定，在具體個案中，開始提供一項服務前可能需要數個同意。

Recital 43 clarifies that consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being

appropriate in the individual case. Recital 32 states "*Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them*".
前言第43點清楚指出，若獲得同意的過程/程序並不允許當事人就個別運用個資行為分別給予同意（例如只同意某些運用行為，不包含其他），儘管在個案中尚屬適當，該同意仍將推定為非自主給予。前言第32點表明「*同意應涵蓋所有基於一個或數個目的之運用行為。當運用行為具有數種目的時，應針對所有的目的都需給予同意*」。

If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific, as discussed in section 3.2 further below. When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.
若控管者將運用行為的數種目的合併，又未就各個目的徵求個別同意時，即缺乏自主性。此區別性與下方第3.2段所述之同意明確性的需求具有緊密關聯。當為追求數種目的而運用個資時，區別性便是符合有效同意條件的解決方案，即數種目的之區分，以及針對個別目的獲得同意。

[Example 7]
Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes, therefore the consent will not be valid. In this case, a specific consent should be collected to send the contact details to commercial partners. Such specific consent will be deemed valid for each partner (see also section 3.3.1), whose identity has been provided to the data subject at the time of the collection of his or her consent, insofar as it is sent to them for the same purpose (in this example: a marketing purpose).

[示例7]
某零售商以同一請求，徵求消費者同意使用其個資於寄送行銷電子郵件，並與集團內其他公司分享消費者資訊。由於無法針對這兩個目的個別表示同意，此同意即不具備區別性，因此不生效力。在本案例中，如要將聯絡資訊寄送予商業夥伴，即應蒐集明確的同意。只有在蒐集當事人之同意時已提供個別夥伴的身分，且係基於相同目的（在本例中：行銷目的）而寄送資訊，則此明確同意對個別夥伴而言才被視為具有效力（並參第3.3.1段）。

#### 3.1.4. Detriment
#### 損害

The controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.
控管者必須證明，拒絕或撤回同意不會導致任何損害（前言第42點）。舉例來說，控管者須證明撤回同意不會對當事人產生任何花費，從而同意之撤回不存有顯著的不利益。

Other examples of detriment are deception, intimidation, coercion or significant negative consequences if a data subject does not consent. The controller should be able to prove that the data subject had a free or genuine choice about whether to consent and that it was possible to withdraw consent without detriment.
其他當事人不予同意而生損害的例子為欺瞞、脅迫、強制或重大負面結果。控管者須能證明當事人對於是否同意享有自主性或真正的選擇權，且可撤回同意而免於任何損害。

If a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was given freely. The GDPR does not preclude all incentives but the onus would be on the controller to demonstrate that consent was still freely given in all the circumstances.

如控管者可證明對某服務得撤回同意而免於任何負面結果時，例如使用者獲得之服務效能不因此而降級，便可能用以證明該同意為自主給予。GDPR並不排除所有獎勵誘因，但控管者有義務證明在任何情況下，同意仍為自主給予。

[Example 8]

When downloading a lifestyle mobile app, the app asks for consent to access the phone's accelerometer. This is not necessary for the app to work, but it is useful for the controller who wishes to learn more about the movements and activity levels of its users. When the user later revokes that consent, she finds out that the app now only works to a limited extent. This is an example of detriment as meant in Recital 42, which means that consent was never validly obtained (and thus, the controller needs to delete all personal data about users' movements collected this way).

[示例8]

下載某生活時尚行動應用程式時，該應用程式要求同意存取手機的加速度計。此非執行應用程式所必要，但有助於控管者更瞭解使用者的移動軌跡和活動程度。當使用者日後撤回該同意時，發現該應用程式僅可在有限範圍內運行。這即是前言第42點所稱損害的適例，表示獲得的同意自始即屬無效（從而，控管者必須將所有以此方式蒐集而跟使用者移動軌跡有關之個人資料刪除）。

[Example 9]

A data subject subscribes to a fashion retailer's newsletter with general discounts. The retailer asks the data subject for consent to collect more data on shopping preferences to tailor the offers to his or her preferences based on shopping history or a questionnaire that is voluntary to fill out. When the data subject later revokes consent, he or she will receive non-personalised fashion discounts again. This does not amount to detriment as only the permissible incentive was lost.

[示例9]

某當事人向時尚產品零售商訂閱一般折扣的產品新訊。該零售商徵求當事人同意蒐集更多購物偏好資料，以便根據其購物歷史或自願填寫的問卷而向其提供符合偏好的產品。當該當事人日後撤回同意時，將再收到非個人化的時尚產品折扣。由於僅損失控管者提供的獎勵誘因，此將不構成損害。

[Example: 10]

A fashion magazine offers readers access to buy new make-up products before the official launch.

The products will shortly be made available for sale, but readers of this magazine are offered an exclusive preview of these products. In order to enjoy this benefit, people must give their postal address and agree to subscription on the mailing list of the magazine. The postal address is necessary for shipping and the mailing list is used for sending commercial offers for products such as cosmetics or t-shirts year round.

The company explains that the data on the mailing list will only be used for sending merchandise and paper advertising by the magazine itself and is not to be shared with any other organisation.

In case the reader does not want to disclose their address for this reason, there is no detriment, as the products will be available to them anyway.

[示例10]

某時尚雜誌提供其讀者在產品正式發表前即可購買化妝新品。

該產品隨後即將上市，但此雜誌的讀者可獨家預覽這些產品。為了享受這項優惠，人們必須提供郵寄地址，並同意列於該雜誌的訂閱者郵寄清單。郵寄地址是為寄送所必要，而郵寄清單是用來每年寄送例如化妝品或短衫等產品的商業資訊。

該公司解釋，郵寄清單上的資料將僅用於寄送產品以及該雜誌自己的紙本廣告，且不會與任何其他組

織分享。
鑒於讀者最終仍可購買該產品，因此如讀者不願基於此原因揭露地址，將不致受到任何損害。

### 3.2. Specific
### 特定性

Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them.[26] The requirement that consent must be '*specific'* aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of 'informed' consent. At the same time it must be interpreted in line with the requirement for 'granularity' to obtain 'free' consent.[27] In sum, to comply with the element of 'specific' the controller must apply:

(i) Purpose specification as a safeguard against function creep,
(ii) Granularity in consent requests, and
(iii) Clear separation of information related to obtaining consent for data processing activities from information about other matters.

第6條第1項第a款確認當事人的同意必須針對「一個或數個特定的」目的而給予，且當事人對個別目的均有選擇權[26]。同意必須「特定」的規範，是為確保當事人擁有一定程度的使用者控制權及透明度。GDPR並未變更此要求，仍密切與「知情」同意的規範連結。同時，解釋上須符合取得「自主」同意的「區別性」要求[27]。簡言之，控管者必須遵守下列條件以符合「特定」的要素：

(i) 目的特定性作為避免用途悄悄擴散的保障，
(ii) 要求之同意須有區別性，以及
(iii) 清楚區分要求同意個資運用行為的資訊與其他事項的資訊。

**Ad. (i):** Pursuant to Article 5(1)(b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.[28] The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.

**補充 (i)：**依GDPR第5條第1項第b款規定，獲得有效同意係以針對有意運用之行為確定其特定、清楚且正當之目的為前提[28]。在當事人同意對於資料的原始蒐集行為後，第5條第1項第b款結合特定同意的要求及目的限制之概念，以此作為避免資料運用之目的逐漸擴大或模糊的保障。此現象亦稱為用途悄悄擴散，由於可能導致控管者或第三人在預期之外使用個資或使

[26] Further guidance on the determination of 'purposes' can be found in Opinion 3/2013 on purpose limitation (WP 203).
關於確定「目的」的進一步指引可見於3/2013關於目的限制之意見書（WP203）。

[27] Recital 43 GDPR states that separate consent for different processing operations will be needed wherever appropriate. Granular consent options should be provided to allow data subjects to consent separately to separate purposes.
GDPR前言第43點謂無論適當與否，都必須能對不同的運用行為分別同意。應向當事人提供可分別同意各個目的之區別同意的選項。

[28] See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 16, : "For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'."
見WP293/2013關於目的限制之意見書（WP203），第16頁，：「基於這些理由，一個模糊或概括的目的，例如沒有其他細節的『優化使用者體驗』、『行銷目的』、『資訊安全目的』或『將來之研究』等，通常無法符合『特定』的標準」。

當事人失去控制權，對當事人將構成風險。

If the controller is relying on Article 6(1)(a), data subjects must always give consent for a specific processing purpose.[29] In line with the concept of *purpose limitation*, Article 5(1)(b) and recital 32, consent may cover different operations, as long as these operations serve the same purpose. It goes without saying that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.
如控管者依循第6條第1項第a款，則當事人須針對特定的運用目的給予同意[29]。根據第5條第1項第b款及前言第32點的*目的限制*觀念，只要這些行為均基於相同目的，同意之標的可以涵蓋不同行為。顯而易見的是，只有在當事人明確知悉使用其個資之預期目的時，才可獲得特定同意。

Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data based on consent and wishes to process the data for another purpose, too, that controller needs to seek additional consent for this other purpose unless there is another lawful basis which better reflects the situation.
儘管對於目的間的相容性設有規範，同意仍須針對特定目的而為。當事人僅在瞭解自己享有控制權，且其個資僅會基於那些特定目的而被運用時，才會給予其同意。在控管者基於同意而運用個資，但又要為其他目的而運用該個資時亦然，即控管者必須就其他的目的另行徵求同意，除非該情形有其他合法基礎可茲適用。

> [Example 11] A cable TV network collects subscribers' personal data, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits. After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber's viewing habits. Given this new purpose, new consent is needed.
> [示例11]某有線電視網基於訂戶同意而蒐集訂戶的個人資料，依訂戶的收視習慣針對新上架電影向訂戶提出個人化建議。一段時間後，該電視網決定要讓第三方按訂戶的收視習慣寄送（或播送）精準廣告。為了這個新目的，必須獲得新的同意。

**Ad. (ii):** Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.
**補充(ii)：**同意機制不僅須有區別性以符合「自主」的規範，也須符合「特定」之要素。此表示為不同目的徵求同意的控管者，應就各個目的提供個別的「選擇加入」選項，以供使用者就特定目的給予特定同意。

**Ad. (iii):** Lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement that controllers must provide clear information, as discussed in paragraph 3.3. below.

[29] This is consistent with WP29 Opinion 15/2011 on the definition of consent (WP 187), for example on p. 17.
此與15/2011關於同意的定義之意見書（WP187）相符，例如第17頁。

**補充(iii)：**最後，為讓當事人知悉不同選擇將造成的影響，控管者應就所徵求個別同意以運用個資之各個目的，分別提供特定資訊。如此，當事人方能給予特定同意。本議題與接下來3.3所要討論的控管者應提供清楚資訊之規範有所重疊。

### 3.3. Informed
### 知情性

The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.

GDPR強化知情同意的規範。依GDPR第5條規定，透明化的要求是基本原則之一，且與公平性及合法性原則密切相關。為了讓當事人得在知情前提下作出決定，瞭解自己同意的內容，並行使例如撤回同意的權利，在獲得其同意前事先提供資訊極為重要。若控管者未提供可取得的資訊，使用者控制權即形同虛設，而同意便成為無效的運用個資依據。

The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.

未符合知情同意規範的結果將導致同意不生效力，而控管者將可能違反GDPR第6條之規定。

#### 3.3.1. Minimum content requirements for consent to be 'informed'
#### 知情同意之內容的最低要求

For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, WP29 is of the opinion that at least the following information is required for obtaining valid consent:

(i) the controller's identity,[30]

(ii) the purpose of each of the processing operations for which consent is sought,[31]

(iii) what (type of) data will be collected and used,[32]

(iv) the existence of the right to withdraw consent,[33]

(v) information about the use of the data for automated decision-making in accordance with Article 22 (2)(c)[34] where relevant, and

(vi) on the possible risks of data transfers due to absence of an adequacy decision and of

[30] See also Recital 42 GDPR: " […]For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.[…]." 30見GDPR前言第42點：「[…]要使同意為知情，當事人應至少知悉控管者的身分及所欲運用個人資料行為之目的[…]」。

[31] Again, see Recital 42 GDPR
同樣見GDPR前言第42點

[32] See also WP29 Opinion 15/2011 on the definition of consent (WP 187) pp.19-20
見WP29意見15/2011關於同意的定義（WP187），第19頁至第20頁

[33] See Article 7(3) GDPR
見GDPR第7條第3項

[34] See also WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), paragraph IV.B, p. 20 onwards.
見WP29關於為2016/679號規則之目的的自動化個別決策與建檔指引（WP251），第IV.B段，第20頁以下。

appropriate safeguards as described in Article46.[35]

為使同意具備知情性，必須將某些對作出決定至為重要的要素告知當事人。因此，WP29認為，至少應將下列資訊作為告知內容，以獲得有效同意：

(i) 控管者的身分[30]，
(ii) 徵求同意的各個運用行為之目的[31]，
(iii) 蒐集與利用之個資（類別）為何[32]，
(iv) 有權撤回同意[33]，
(v) 涉及第22條第2項第c款規定[34]時提供關於利用個資以作出自動化決策的資訊，以及
(vi) 依第46條所述[35]，告知因未取得適足性決定且未有適當安全維護措施而傳輸個資的潛在風險。

With regard to item (i) and (iii), WP29 notes that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named. Processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors. To conclude, WP29 notes that depending on the circumstances and context of a case, more information may be needed to allow the data subject to genuinely understand the processing operations at hand.

WP29就上述項目(i)及(iii)提到，在由多數（聯合）控管者徵求同意的案例中，或個資將傳輸予其他控管者或由其他控管者運用，而這些控管者均以原始同意作為法律依據的情形，這些組織的名稱都應揭露。雖然依GDPR第13條及第14條規定，控管者必須提供包含受託運用者在內的個資接受者完整名單或接受者類別，但同意的規範並不要求事先揭露受託運用者之名稱。總之，WP29表示，依個案情形與背景不同，可能須要提供更多的資訊，以便讓當事人真正瞭解即將發生的運用行為。

### 3.3.2. How to provide information
### 提供資訊的方式

The GDPR does not prescribe the form or shape in which information must be provided in order to fulfil the requirement of informed consent. This means valid information may be presented in various ways, such as written or oral statements, or audio or video messages. However, the GDPR puts several requirements for informed consent in place, predominantly in Article 7(2) and Recital32. This leads to a higher standard for the clarity and accessibility of the information.

GDPR並未就滿足知情同意之規範而對提供資訊的格式或形式有所規定。這表示得以不同方式呈現有效的資訊，例如書面或言詞聲明，或聲音或影像訊息。然而，GDPR對知情同意訂有數項規範，主要規定於第7條第2項及前言第32點，為資訊的清晰性與可得性設下更高的標準。

When seeking consent, controllers should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long privacy policies that are difficult to understand or statements

[35] Pursuant to Article 49 (1)(a), specific information is required about the absence of safeguards described in Article 46, when explicit consent is sought. See also WP29 Opinion 15/2011 on the definition of consent (WP 187)p. 19
依第49條第1項第a款規定，在尋求明確同意時，須提供關於不具備第46條所述的安全維護之特定資訊。見WP29意見15/2011關於同意的定義（WP187），第19頁

full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions.[36]
在徵求同意時，控管者應確保在任何情況均使用清楚且簡白的語言。這代表該訊息不僅對律師，對一般人來說，也應可輕易理解。控管者不可採用冗長而難以理解的隱私權政策或充滿法律用語的聲明。同意必須清晰且可與其他事項有所區隔，並以可理解且可輕易取得的方式提供。此規範實質上表示，不可將與同意與否的知情決定有關之資訊隱藏於一般的條款與條件中[36]。

A controller must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the controller is and to understand what they are agreeing to. The controller must clearly describe the purpose for data processing for which consent is requested.[37]
控管者必須確保同意是以「能讓當事人輕易識別控管者身分，並瞭解其所同意的內容為何之資訊」為基礎而提供。控管者須就所尋求同意之個資運用行為清楚描述其目的[37]。

Other specific guidance on the accessibility has been provided in the WP29 guidelines on transparency. If consent is to be given by electronic means, the request must be clear and concise. Layered and granular information can be an appropriate way to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand.
WP29曾發布關於透明化的指引，對可得性提出其他具體指引。如以電子方式給予同意時，其請求必須清楚而簡潔。階層式及區別性資訊可作為因應「準確且完整」及「可理解性」此雙重義務的適當作法。

A controller must assess what kind of audience it is that provides personal data to their organisation. For example, in case the targeted audience includes data subjects that are underage, the controller is expected to make sure information is understandable for minors.[38] After identifying their audience, controllers must determine what information they should provide and, subsequently how they will present the information to data subjects.
控管者必須評估向其組織提供個人資料之受眾種類。例如，目標受眾包含尚未成年之當事人，則控管者應確保未成年人亦可瞭解其資訊[38]。在識別受眾後，控管者必須決定要提供何種資訊，再決定如何向當事人提出該資訊。

Article 7(2) addresses pre-formulated written declarations of consent which also concern other matters. When consent is requested as part of a (paper) contract, the request for consent should be clearly distinguishable from the other matters. If the paper contract includes many aspects that are unrelated to the question of consent to the use of personal data, the issue of consent should be dealt with in a way that clearly stands out, or in a separate document. Likewise, if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a

[36] The declaration of consent must be named as such. Drafting, such as "I know that…" does not meet the requirement of clear language.
同意的聲明必須表示其為同意。以例如「我知悉…」為文並不符合清楚的語言之規範。
[37] See Articles 4(11) and 7(2) GDPR.
見GDPR第4條第11款及第7條第2項。
[38] See also Recital 58 regarding information understandable for children.
見前言第58點有關兒童可理解之資訊。

paragraph within terms and conditions, pursuant to Recital 32.[39] To accommodate for small screens or situations with restricted room for information, a layered way of presenting information can be considered, where appropriate, to avoid excessive disturbance of user experience or product design.
第7條第2項提出的定型化書面同意聲明也涉及其他議題。當同意的請求是（書面）契約的一部分時，該請求應清楚與其他事項區別。如書面契約包含與同意使用個人資料無關的許多面向時，對於同意事項應清楚突顯，或呈現於另一份文件。同樣的，如經由電子方式徵求同意，該同意之請求應分列並有所區別，依前言第32點規定[39]，不可僅作為條款與條件的一個段落。考慮到小螢幕或僅在有限空間揭露資訊的情形，可於適當時機，考慮採用階層方式呈現資訊，以避免對使用者體驗或產品設計造成過度干擾。

A controller that relies on consent of the data subject must also deal with the separate information duties laid down in Articles 13 and 14 in order to be compliant with the GDPR. In practice, compliance with the information duties and compliance with the requirement of informed consent may lead to an integrated approach in many cases. However, this section is written in the understanding that valid "informed" consent can exist, even when not all elements of Articles 13 and/or 14 are mentioned in the process of obtaining consent (these points should of course be mentioned in other places, such as the privacy notice of a company). WP29 has issued separate guidelines on the requirement of transparency.
為符合GDPR要求，以當事人同意作為法律依據的控管者，也應因應第13條和第14條規定的個別資訊揭露之義務。實務上，許多案例可能以整合方式，同時遵守資訊揭露義務及知情同意規範。然而，本段是以「即便獲得同意的過程未揭露所有第13條與/或第14條中的要素（但這些要素務必應在其他地方提出，例如公司的隱私聲明），但有效的『知情』同意仍可存在」為理解前提。WP29已就透明化的要求發布另一份指引。

> [Example 12]
> Company X is a controller that received complaints that it is unclear to data subjects for what purposes of data use they are asked to consent to. The company sees the need to verify whether its information in the consent request is understandable for data subjects. X organises voluntary test panels of specific categories of its customers and presents new updates of its consent information to these test audiences before communicating it externally. The selection of the panel respects the principle of independence and is made on the basis of standards ensuring a representative, non-biased outcome. The panel receives a questionnaire and indicates what they understood of the information and how they would score it in terms of understandable and relevant information. The controller continues testing until the panels indicate that the information is understandable. X draws up a report of the test and keeps this available for future reference. This example shows a possible way for X to demonstrate that data subjects were receiving clear information before consenting to personal data processing by X.
> [示例12]
> X公司為控管者，收到「當事人不清楚該公司要求同意利用個資的目的」之申訴。該公司認為有需要查明當事人是否理解該公司在要求同意時提供的資訊。X依客戶分類組成自願受測小組，並在對外公布之前，將更新的同意資訊提供給這些受測人員。小組人員的挑選符合獨立性原則，並且基於確保產出結果的代表性及不帶偏見之標準。該小組收到問卷並寫下其對資訊的理解，以及對於資訊的可理解性與關聯性如何評分。控管者持續進行測試，直到小組表明該資訊已可理解。X將測試結果製成報告並保存作為未來的參考。此示例即展示X得以證明「當事人在同意X運用個資之前，已獲得清楚資訊」

[39] See also Recital 42 and Directive 93/13/EC, notably Article 5 (plain intelligible language and in case of doubt, the interpretation will be in favour of consumer) and Article 6 (invalidity of unfair terms, contract continues to exist without these terms only if still sensible, otherwise the whole contract is invalid).
見前言第42點及第93/13/EC號指令，特別是第5條（簡白可理解之語言，且如有疑義，從有利於消費者之解釋）及第6條（部分條款因不公平而無效時，契約僅在除去該條款仍屬合理時始繼續有效，否則全部契約均歸無效）。

的可能方式。

[Example 13]
A company engages in data processing on the basis of consent. The company uses a layered privacy notice that includes a consent request. The company discloses all basic details of the controller and the data processing activities envisaged.[40] However, the company does not indicate how their data protection officer can be contacted in the first information layer of the notice. For the purposes of having a valid lawful basis as meant in Article 6, this controller obtained valid "informed" consent, even when the contact details of the data protection officer have not been communicated to the data subject (in the first information layer), pursuant to Article 13(1)(b) or 14(1)(b)GDPR.
[示例13]
某公司以同意為法律依據而運用個人資料。該公司使用階層式隱私聲明，其中包含要求給予同意。該公司揭露控管者的所有基本細節以及規劃的個資運用行為[40]。然而，該公司在聲明的第一層資訊中並未說明如何聯繫其資料保護長。基於第6條以獲得有效合法基礎為目的之規範意旨，即便未依GDPR第13條第1項第b款或第14條第1項第b款向當事人（在第一層資訊）提供資料保護長的聯絡方式，該控管者仍已取得有效的「知情」同意。

### 3.4. Unambiguous indication of wishes
### 非模糊的意思表示

The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.
GDPR明確要求同意須有當事人的聲明或清楚肯定行為，此表示同意須經由積極行動或聲明而提出。當事人對特定運用行為之同意須足夠明顯。

Article 2(h) of Directive 95/46/EC described consent as an "indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed". Article 4(11) GDPR builds on this definition, by clarifying that valid consent requires an *unambiguous* indication by means of a *statement or by a clear affirmative action*, in line with previous guidance issued by the WP29.
95/46/EC指令第2條第h款將同意描述為一個「當事人為表明同意運用與其有關之個人資料而作出的意思表示」。GDPR第4條第11款即以此定義為基礎，說明有效同意須有一個透過*聲明或清楚肯定行為*所為的*非模糊*表示，此與WP29之前發布的指引相符。

A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing.[41] Recital 32 sets out additional guidance on this. Consent can be

[40] Note that when the identity of the controller or the purpose of the processing is not apparent from the first information layer of the layered privacy notice (and are located in further sub-layers), it will be difficult for the data controller to demonstrate that the data subject has given informed consent, unless the data controller can show that the data subject in question accessed that information prior to giving consent.
當控管者的身分或運用行為的目的在階層式隱私聲明的第一層資訊並不明顯時（記載於下一層），除非資料控管者可證明該當事人在給予同意前已存取該資訊，否則資料控管者將難以證明當事人已給予知情同意。

[41] See Commission Staff Working Paper, Impact Assessment, Annex 2, p. 20 and also pp. 105-106: "As also pointed out in the opinion adopted by WP29 on consent, it seems essential to clarify that valid consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent, while making clear that – in the context of the on-line environment – the use of default options which the data subject is required to modify in order to reject the processing ('consent based on silence') does not in itself constitute unambiguous consent. This would give individuals more control over their own data, whenever processing is based on his/her consent. As regards impact on data controllers, this would not have a major impact as it solely clarifies and better spells out the implications of the current Directive in relation to the conditions for a valid and meaningful consent from the data subject. In particular, to the extent that 'explicit' consent would clarify – by replacing "unambiguous" – the modalities and quality of consent and that it is not intended to extend the cases and situations where (explicit) consent should be used as a ground for processing, the impact of this measure on data controllers

collected through a written or (a recorded) oral statement, including by electronic means.
一個「清楚肯定的行為」代表當事人必須在慎重考慮後，以行動對特定運用行為表示同意[41]。前言第32點對此有額外指引。同意之蒐集可經由書面或（經記錄的）口頭聲明，包含以電子方式為之。

Perhaps the most literal way to fulfil the criterion of a "written statement" is to make sure a data subject writes in a letter or types an email to the controller explaining what exactly he/she agrees to. However, this is often not realistic. Written statements can come in many shapes and sizes that could be compliant with the GDPR.
或許最符合「書面聲明」文義的標準方式即是確保當事人將其同意的內容於書面或電子郵件中寫下以交付控管者。然而這通常不夠實際。書面聲明可以多種形式和尺寸符合GDPR的要求。

Without prejudice to existing (national) contract law, consent can be obtained through a recorded oral statement, although due note must be taken of the information available to the data subject, prior to the indication of consent. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.
在不牴觸現行（國家）契約法的前提下，雖然在當事人表示同意之前，必須充分註明當事人可得之資訊，但同意可藉由經記錄之口頭聲明而獲得。在GDPR下，使用預先勾選同意加入的框格是無效的。當事人的單純沉默、不作為或繼續使用服務之行為，均不可視為對其選擇的積極表示。

> [Example 14]
> When installing software, the application asks the data subject for consent to use non-anonymised crash reports to improve the software. A layered privacy notice providing the necessary information accompanies the request for consent. By actively ticking the optional box stating, "I consent", the user is able to validly perform a ´clear affirmative act´ to consent to the processing.
> [示例14]
> 在安裝軟體時，應用程式要求當事人同意利用非匿名的當機報告以優化軟體。階層式隱私聲明提供包含同意之請求在內的必要資訊。藉由主動勾選「我同意」的框格，使用者即可有效作出一個「清楚肯定的行為」以同意運用個資。

A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes').[42]

---

is not expected to be major."
見執委會工作文件，衝擊評估，附錄2，第20頁及第105頁至第106頁：「正如WP29通過關於同意的意見書同樣指出，有必要明確說明的是，有效同意需採用對當事人之同意意思不會存有懷疑的機制，且清楚說明在線上環境中，讓當事人須更改設定才可拒絕運用的預設選項（『基於沉默的同意』），其本身並不構成非模糊的同意。此將使個人在控管者基於其同意而運用資料時，對其資料有更多的控制權。至於對資料控管者的衝擊方面，由於此僅澄清並更詳細說明現行指令關於當事人有效且有意義之同意的意旨，此將不會有重大影響。特別是取代『非模糊』的『明確』同意一詞僅在說明同意的形式與品質，且無意擴大以（明確）同意作為運用依據的適用情形，因此此方式對資料控管者的衝擊應不重大」。

[42] See Article 7(2). See also Working Document 02/2013 on obtaining consent for cookies (WP 208), pp. 3-6.
見第7條第2項。亦見02/2013關於為cookies獲取同意之工作文件（WP208），第3頁至第6頁。

控管者也應留意，同意不可經由「同意某契約或接受某服務之一般條款與條件所為的同一行為」而取得。對一般條款與條件的空白接受，不可視為同意使用個人資料的清楚肯定行為。GDPR並不允許控管者提出讓當事人要有介入行為才可免於同意（例如「選擇退出框格」）的預先勾選框格或選擇退出架構[42]。

When consent is to be given following a request by electronic means, the request for consent should not be *unnecessarily* disruptive to the use of the service for which the consent is provided.[43] An active affirmative motion by which the data subject indicates consent can be necessary when a less infringing or disturbing modus would result in ambiguity. Thus, it may be necessary that a consent request interrupts the use experience to some extent to make that request effective.
當同意是經電子方式之請求而給予時，該請求不可*非必要地*造成服務使用上的干擾[43]。如果較低侵擾或干擾的方式將導致意義不明的話，當事人以積極肯定的行為表達同意即有必要。因此，為使同意的請求發生效力，可能有必要在某種程度上干擾使用體驗。

However, within the requirements of the GDPR, controllers have the liberty to develop a consent flow that suits their organisation. In this regard, physical motions can be qualified as a clear affirmative action in compliance with the GDPR.
然而在GDPR的規範下，控管者可自由發展適合其組織的同意流程。在這點上，身體動作可符合GDPR規範的清楚肯定行為。

Controllers should design consent mechanisms in ways that are clear to data subjects. Controllers must avoid ambiguity and must ensure that the action by which consent is given can be distinguished from other actions. Therefore, merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation.
控管者應以對當事人足夠清晰的方式設計同意機制。控管者必須避免任何模糊空間，並確保給予同意之行為可與其他行為有所區別。因此，僅是持續一般的使用網站並不可推論為當事人對運用行為表達同意的意思表示。

[Example 15]
Swiping a bar on a screen, waiving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g. if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm). The controller must be able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given.
[示例15]
只要已提供清楚的資訊，且該動作可清楚表明對特定請求的同意（例如將捲軸滑至左方，即表示同意基於Y目的而利用X資訊。重複該動作以確認），則滑動螢幕上的捲軸、在智慧鏡頭前揮手、將智慧型手機順時鐘或八字形旋轉，均是表示同意的選項。控管者必須證明以此方式獲得同意，且當事人可以同樣簡易方式撤回同意。

[Example 16]
Scrolling down or swiping through a website will not satisfy the requirement of a clear and affirmative action.

[43] See Recital 32 GDPR.
見GDPR前言第32點。

This is because the alert that continuing to scroll will constitute consent may be difficult to distinguish and/or may be missed when a data subject is quickly scrolling through large amounts of text and such an action is not sufficiently unambiguous.

[示例16]

下捲或滑過網站無法滿足清楚及肯定行動的要求。這是因為對於繼續瀏覽即構成同意的警示可能不易辨認，且/或在當事人快速瀏覽大量文字時恐遭忽略，進而使該行為有模糊空間。

In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.

在數位環境下，許多服務需要個人資料以提供功能，因此，當事人每天收到多個需要點擊或滑動以回覆的同意請求。這可能造成某程度的點擊疲勞：即遇到越多次時，同意機制真正的警示效果就越趨減損。

This results in a situation where consent questions are no longer read. This is a particular risk to data subjects, as, typically, consent is asked for actions that are in principle unlawful without their consent. The GDPR places upon controllers the obligation to develop ways to tackle this issue.

這導致大家不再閱讀關於同意的提問。此對當事人尤其是個風險，因為在典型的情況，徵求同意是為了未獲得同意即屬違法的行為。GDPR課予控管者想出方法以茲因應的義務。

An often-mentioned example to do this in the online context is to obtain consent of Internet users via their browser settings. Such settings should be developed in line with the conditions for valid consent in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers.

對此，線上環境有個常被提及的因應實例，即經由瀏覽器設定以取得網路使用者的同意。此類設定應遵循GDPR對於有效同意的條件而設計，例如同意應分別針對各個預想的目的，以及提供的資訊中應包含控管者的名稱。

In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed. WP29 has consistently held in previous opinions that consent should be given prior to the processing activity.[44] Although the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording "has given" in Article 6(1)(a) support this interpretation. It follows logically from Article 6 and Recital 40 that a valid lawful basis must be present before starting a data processing. Therefore, consent should be given prior to the processing activity. In principle, it can be sufficient to ask for a data subject's consent once. However, controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged.

無論如何，如獲得同意是控管者運用個人資料所必須，控管者應在運用個資之前取得該同意。WP29在先前的意見中一致地認為，同意應在運用行為之前提供[44]。雖然GDPR在第4條第11款的文字中並未規定同意須在運用行為之前給予，但已清楚揭示此意。第6條第1項的條文名稱以及第6條第1項第a款的文字「已給予」即足支持此解釋。由第6條及前言第40點的邏輯推

[44] WP29 has consistently held this position since Opinion 15/2011 on the definition of consent (WP 187), pp. 30-31.
WP29自15/2011關於同意的定義之意見書（WP187），第30頁至第31頁以來一貫保持此見解。

演可知，有效的合法基礎必須在開始運用個資之前即已存在。因此，同意應在運用行為之前給予。原則上，向當事人請求一次同意即為已足。然而，控管者如在取得同意後變更運用個資之目的，或規劃額外的目的時，即須取得一個新的特定同意。

### 4. Obtaining explicit consent
### 獲得明確同意

Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49[45] , and in Article 22 on automated individual decision-making, including profiling.[46]
在有重大個資保護風險情形出現時，明確同意有其必要，因此，宜針對個人資料提供高度個人掌控權。在GDPR規範下，明確同意出現在第9條關於特種個資的運用、第49條關於在缺少充分防護措施的情形下，將個資傳輸至第三國或國際組織的規範[45]，以及第22條關於包含建檔在內的自動化個人決定[46]等條文中。

The GDPR prescribes that a "statement or clear affirmative action" is a prerequisite for 'regular' consent. As the 'regular' consent requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the *explicit* consent of a data subject in line with the GDPR.
GDPR將「聲明或清楚肯定的行動」規定為「一般」同意的必要條件。由於GDPR對於「一般」同意的規範相較95/46/EC指令已有更高標準，因此有必要澄清控管者應採取何種額外措施獲得當事人的*明確*同意以符合GDPR。

The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.[47]

---

[45] According to Article 49 (1)(a) GDPR, explicit consent can lift the ban on data transfers to countries without adequate levels of data protection law. Also note Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114), p. 11, where WP29 has indicated that consent for data transfers that occur periodically or on an on-going basis is inappropriate.
依GDPR第49條第1項第a款規定，明確同意可解除禁止將資料傳輸至不具備適足程度之資料保護法律的國家。也留意關於1995年10月24日之95/46/EC指令第26條第1項的共通解釋之工作文件（WP114），第11頁，WP29在此指出，以同意作為對週期性或持續性的資料傳輸之依據並不恰當。

[46] In Article 22, the GDPR introduces provisions to protect data subjects against decision-making based solely on automated processing, including profiling. Decisions made on this basis are allowed under certain legal conditions. Consent plays a key role in this protection mechanism, as Article 22(2)(c) GDPR makes clear that a controller may proceed with automated decision making, including profiling, that may significantly affect the individual, with the data subject's explicit consent. WP29 have produced separate guidelines on this issue: WP29 Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017 (WP 251).
在第22條中，GDPR提出保護當事人免於僅根據自動化運用行為（包含建檔）而作出決定之條款。在特定條件下才可依此作出決定。同意在這個保護機制中扮演重要角色，即GDPR第22條第2項第c款清楚規定控管者可根據當事人的明確同意而採行對個人可能有重要影響的自動化決定，包含建檔。WP29對此議題個別提出指引：WP29關於依第2016/679號規則之目的的自動化決定與建檔之指引，2017年10月3日（WP251）。

[47] See also WP29 Opinion 15/2011, on the definition of consent (WP 187), p. 25.
見WP29 15/2011意見書關於同意的定義（WP187），第25頁。

*明確*一詞涉及當事人表達同意的方式。此代表當事人必須作出明確聲明來表示同意。確保同意明確的一種明顯方式是藉由書面聲明明確地確認其同意。在適當的情形下，控管者可確保當事人在該書面聲明中簽名，以避免所有可能的質疑及將來潛在無法舉證的情況[47]。

However, such a signed statement is not the only way to obtain explicit consent and, it cannot be said that the GDPR prescribes written and signed statements in all circumstances that require valid explicit consent. For example, in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, the use of oral statements can also be sufficiently express to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded.

然而，簽名的聲明並非取得明確同意的唯一方式，且GDPR並未規定在所有需要有效的明確同意之情形，都要有書面簽名的聲明。舉例來說，在數位或線上環境下，當事人可透過填寫電子表格、寄送電子郵件、上傳包含當事人簽名在內的掃描後文件，或使用電子簽章以提交所需的聲明。理論上，口頭聲明對於取得有效的明確同意也足夠明確，不過，控管者在記錄該聲明時，可能不易舉證已符合所有有效的明確同意之條件。

An organisation may also obtain explicit consent through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject (e.g. pressing a button or providing oral confirmation).

只要相關選項的資訊足夠公平、可理解、夠清楚，且向當事人要求具體的確認動作（例如按下按鈕或提供口頭確認），組織也可經由電話對話而獲得明確同意。

> [Example 17] A data controller may also obtain explicit consent from a visitor to its website by offering an explicit consent screen that contains Yes and No check boxes, provided that the text clearly indicates the consent, for instance "I, hereby, consent to the processing of my data", and not for instance, "It is clear to me that my data will be processed". It goes without saying that the conditions for informed consent as well as the other conditions for obtaining valid consent should be met.
> [示例17]藉由在獲得明確同意的螢幕上提供是、否勾選框格，只要文字清楚指出同意，例如「我在此同意對我的個人資料之運用行為」，而非例如「我清楚我的個人資料將被運用」，則資料控管者也可以此獲得網站訪客的明確同意。但仍須符合知情同意及其他獲得有效同意之條件，自不待言。

> [Example 18] A clinic for cosmetic surgery seeks explicit consent from a patient to transfer his medical record to an expert whose second opinion is asked on the condition of the patient. The medical record is a digital file. Given the specific nature of the information concerned, the clinic asks for an electronic signature of the data subject to obtain valid explicit consent and to be able to demonstrate that explicit consent was obtained.[48]
> [示例18]某整形診所為向專家就病人的情況尋求第二意見而請求病人明確同意傳輸其醫療紀錄。該醫療紀錄為數位檔案。考量該資訊的特定性質，該診所要求當事人提供電子簽章以獲得有效的明確同意，並可證明已取得該明確同意[48]。

Two stage verification of consent can also be a way to make sure explicit consent is valid. For example, a data subject receives an email notifying them of the controller's intent to process a

[48] This example is without prejudice to EU Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
此示例不牴觸歐洲議會與歐盟理事會2014年7月23日關於內部市場電子交易之電子身分驗證及信賴服務的歐盟規則（EU）第910/2014號。

record containing medical data. The controller explains in the email that he asks for consent for the use of a specific set of information for a specific purpose. If the data subjects agrees to the use of this data, the controller asks him or her for an email reply containing the statement 'I agree'. After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement.
雙階段驗證同意也可作為確保明確同意之有效性的方式。舉例來說，當事人收到一封電子郵件通知信，說明控管者有意運用包含醫療資料在內的紀錄。該控管者在信中解釋，其基於特定目的而請求同意使用特定的資訊。如當事人同意其使用個人資料，控管者要求以電子郵件回覆「我同意」之聲明。當事人在寄出回覆後，即收到必須點選的驗證連結，或含有驗證碼在內的簡訊，以此確認同意。

Article 9(2) does not recognize "necessary for the performance of a contract" as an exception to the general prohibition to process special categories of data. Therefore controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). Should none of the exceptions (b) to (j) apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data.
第9條第2項未將「為履行契約所必要」列為禁止運用特種個資的例外條款。因此控管者及成員國對此應探究第9條第2項第b款至第j款的特殊例外規定。若第b款至第j款均不適用時，遵守GDPR對有效同意之條件以獲得明確同意，將成為運用該類個資唯一可能的合法例外。

[Example 19]
An airline company, Holiday Airways, offers an assisted travelling service for passengers that cannot travel unassisted, for example due to a disability. A customer books a flight from Amsterdam to Budapest and requests travel assistance to be able to board the plane. Holiday Airways requires her to provide information on her health condition to be able to arrange the appropriate services for her (hence, there are many possibilities e.g. wheelchair on the arrival gate, or an assistant travelling with her from A to B.) Holiday Airways asks for explicit consent to process the health data of this customer for the purpose of arranging the requested travel assistance. -The data processed on the basis of consent should be necessary for the requested service. Moreover, flights to Budapest remain available without travel assistance. Please note that since that data are necessary for the provision of the requested service, Article 7 (4) does not apply.
[示例19]
假期航空公司為無法自行旅行的乘客（例如因為身心障礙）提供旅行協助服務。某顧客預訂從阿姆斯特丹飛往布達佩斯的航班，並要求提供旅行協助以順利登機。假期航空要求該顧客提供關於健康情形的資訊以妥善安排服務（因此有許多選項，例如接機口的輪椅或從阿姆斯特丹到布達佩斯的陪伴飛行助手）。假期航空基於安排旅行協助的目的而要求該顧客給予運用健康資料的明確同意。基於同意而運用之個人資料對於所要求的服務應有必要。此外，飛往布達佩斯但不提供旅行協助的航班仍有空位。請留意，既然該個人資料對所要求提供的服務係屬必要，第7條第4項在此即不適用。

[Example 20]
A successful company is specialised in providing custom-made ski- and snowboard goggles, and other types of customised eyewear for outdoors sports. The idea is that people could wear these without their own glasses on. The company receives orders at a central point and delivers products from a single location all across the EU. In order to be able to provide its customised products to customers who are short-sighted, this controller requests consent for the use of information on customers' eye condition. Customers provide the necessary health data, such as their prescription data online when they place their order. Without this, it is not possible to provide the requested customized eyewear. The company also offers series of goggles with standardized correctional values. Customers that do not wish to share health data could opt for the standard versions.

Therefore, an explicit consent under Article 9 is required and consent can be considered to be freely given.

[示例20]

某間成功的公司專門提供客製化的滑雪板及護目鏡，以及其他類型客製化戶外運動眼鏡。人們戴上該公司產品即不用再戴自己的眼鏡。該公司集中接受訂單，並從單一據點向全歐盟寄送產品。為提供客製產品給近視的顧客，該控管者要求同意使用關於顧客視力情況的資訊。顧客在線上下訂時提供了必要的健康資料，例如處方資料。如果沒有此類資料，將無法提供所要求的客製化眼鏡。該公司同時提供一系列標準度數的護目鏡。不願分享健康資料的顧客可以選擇標準版產品。因此，此處須要第9條規定的明確同意，而該同意可視為自由給予。

## 5. Additional conditions for obtaining valid consent
## 獲得有效同意的其他條件

The GDPR introduces requirements for controllers to make additional arrangements to ensure they obtain, and maintain and are able to demonstrate, valid consent. Article 7 of the GDPR sets out these additional conditions for valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent. Article 7 also applies to consent referred to in other articles of GDPR, e.g. Articles 8 and 9. Guidance on the additional requirement to demonstrate valid consent and on withdrawal of consent is provided below.

GDPR規範控管者採取額外措施以確保其獲得、維持，並可證明有效同意。GDPR第7條藉由同意紀錄之保存與輕易撤回同意之權利等特別條款，以訂定這些針對有效同意的額外條件。第7條也適用於GDPR其他涉及同意之條文，例如第8條及第9條。以下即就證明有效同意的額外規範以及關於同意之撤回提供指引。

### 5.1. Demonstrate consent
### 證明同意

In Article 7(1), the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. The burden of proof will be on the controller, according to Article 7(1).

在第7條第1項中，GDPR清楚指出控管者負有證明當事人同意的明確義務。依第7條第1項規定，此應由控管者負舉證責任。

Recital 42 states: *"Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation."*

前言第42點謂：「*當運用的依據為當事人之同意時，控管者須能證明該當事人已對該運用作業給予同意*」。

Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations. At the same time, the duty to demonstrate that valid consent has been obtained by a controller, should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing (to show consent was obtained) but they shouldn't be collecting any more information than necessary.

控管者可採適合其日常作業的方式，自由發展遵循該條款的方法。在此同時，控管者有責任證明其獲得有效同意，但該責任不應導致過量運用其他資料。這表示控管者應有足夠的資料來證明與運用行為之間的連結（證明已獲得同意），但不可在必要範圍外蒐集任何更多的資訊。

It is up to the controller to prove that valid consent was obtained from the data subject. The GDPR

does not prescribe exactly how this must be done. However, the controller must be able to prove that a data subject in a given case has consented. As long as a data processing activity in question lasts, the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer then strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims, in accordance with Article 17(3)(b) and (e).

控管者可決定如何證明已自當事人獲得有效同意。GDPR並未明確規定該如何滿足此義務。然而，控管者須能證明在個案中的當事人已表示同意。只要系爭資料運用行為持續存在，證明同意的義務便持續存在。依第17條第3項第b款及第e款規定，在運用行為終了後，同意證據的保存期限不應超過遵守法律義務或建立、行使或防禦法律上請求所需的嚴格必要範圍。

For instance, the controller may keep a record of consent statements received, so he can show how consent was obtained, when consent was obtained and the information provided to the data subject at the time shall be demonstrable. The controller shall also be able to show that the data subject was informed and the controller´s workflow met all relevant criteria for a valid consent. The rationale behind this obligation in the GDPR is that controllers must be accountable with regard to obtaining valid consent from data subjects and the consent mechanisms they have put in place. For example, in an online context, a controller could retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time. It would not be sufficient to merely refer to a correct configuration of the respective website.

舉例來說，控管者可以保存所收到的同意聲明之紀錄，以便在需要舉證時，證明如何獲得同意、何時獲得同意，以及當時曾提供給當事人的資訊為何。控管者也須能證明當事人的知情，以及控管者的工作流程符合所有有效同意的相關標準。此義務在GDPR中的背後原理在於，控管者對於自當事人獲得有效同意以及其採取的同意機制應負責任。例如，在線上環境中，控管者可將表達同意的連線進程資訊予以保存，併同該連線進程進行時的同意工作流程之文件紀錄，以及當下提供予當事人之資訊的複本（檔）一併保存。僅是提出個別網站的正確組態設定並不足夠。

> [Example 21] A hospital sets up a scientific research programme, called project X, for which dental records of real patients are necessary. Participants are recruited via telephone calls to patients that voluntarily agreed to be on a list of candidates that may be approached for this purpose. The controller seeks explicit consent from the data subjects for the use of their dental record. Consent is obtained during a phone call by recording an oral statement of the data subject in which the data subject confirms that they agree to the use of their data for the purposes of project X.
>
> [示例21]某醫院發起一個名為X計畫的科學研究計畫，需要實際的病人牙科紀錄。該計畫招募參與者的方式為致電病人，詢問是否同意自願加入候選名單，以便依此目的向其聯繫。控管者向當事人尋求明確同意使用牙科紀錄。此同意是經由錄下當事人確認同意為X計畫之目的使用其個資的口頭聲明，而在電話中獲得。

There is no specific time limit in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, then new consent needs to be obtained.

GDPR對於同意的有效期限沒有特別限制。同意的效期應視個案背景、原始同意的範圍以及

當事人的期待而定。如運用作業有相當大的變更或演變，則原本的同意即不再有效。在此情形便須要獲得新的同意。

WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights.[49]
WP29對最佳實務的建議是，同意應適時更新。再次提供全部資訊有助於確保當事人對於其資料如何被使用以及如何行使其權利，能保持良好的知情狀態[49]。

### 5.2. Withdrawal of consent
### 撤回同意

Withdrawal of consent is given a prominent place in the GDPR. The provisions and recitals on withdrawal of consent in the GDPR can be regarded as codification of the existing interpretation of this matter in WP29 Opinions.[50]
同意之撤回在GDPR佔有重要地位。GDPR中關於同意之撤回的條款與前言，可視為是WP29意見中對此議題現有之解釋的彙整[50]。

Article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The GDPR does not say that giving and withdrawing consent must always be done through the same action.
GDPR第7條第3項規定，控管者應確保同意可由當事人以給予同意相同簡易的方式，在任何時間撤回。GDPR並未規定給予和撤回同意必須透過同樣動作完成。

However, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels.[51]
然而，當同意是以一鍵點擊滑鼠、滑動或按鍵等電子方式獲得時，當事人在實作上須可以相同簡易的方式撤回該同意。如同意是藉由使用該服務特定的使用者介面（例如透過網站、應用程式、登入帳號、物聯網裝置的介面或電子郵件）而獲得時，當事人毫無疑問須可以相同的電子介面撤回同意，因為僅是為了撤回同意而須切換至其他介面將需要過度付出。此外，

[49] See WP29 guidelines on transparency. [Citation to be finalized when available]
見WP29關於透明化之指引。[將於可得時確定引註內容]

[50] WP29 has discussed this subject in their Opinion on consent (see Opinion 15/2011 on the definition of consent (WP 187), pp. 9, 13, 20, 27 and 32-33) and, inter alia, their Opinion on the use of location data. (see Opinion 5/2005 on the use of location data with a view to providing value-added services (WP 115), p. 7).
WP29曾於關於同意之意見書（見15/2011關於同意的定義之意見書（WP187），第9頁、第13頁、第20頁、第27頁及第32頁至第33頁）及特別是關於位置資料的使用之意見書（見5/2005關於由提供加值服務的觀點探討位置資料的使用之意見書（WP115），第7頁）中討論此主題。

[51] See also opinion WP29 Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (WP 174) and the Opinion on the use of location data with a view to providing value-added services (WP 115).
見WP29 4/2010關於在行銷中使用個人資料之歐洲FEDMA行為守則之意見書（WP174）以及關於由提供加值服務的觀點探討位置資料的使用之意見書（WP115）。

當事人須可不受損害的撤回同意。這意味控管者尤應盡可能使撤回同意無需付費或不致降低服務水平[51]。

> [Example 22] A music festival sells tickets through an online ticket agent. With each online ticket sale, consent is requested in order to use contact details for marketing purposes. To indicate consent for this purpose, customers can select either No or Yes. The controller informs customers that they have the possibility to withdraw consent. To do this, they could contact a call centre on business days between 8am and 5pm, free of charge. The controller in this example does not comply with article 7(3) of the GDPR. Withdrawing consent in this case requires a telephone call during business hours, this is more burdensome than the one mouse-click needed for giving consent through the online ticket vendor, which is open 24/7.
>
> [示例22]某音樂節透過線上票券代理商銷售門票。在每一次線上販售票券時，均針對基於行銷目的利用其聯絡方式，尋求(顧客)同意。針對此目的，顧客可選擇不同意或同意，且控管者通知顧客有權撤回同意，如欲行使該權利，可在營業日的早上8點到下午5點間致電客服中心，不須給付任何費用。本例中的控管者並未符合GDPR第7條第3項規定。在本例中，相較於24小時均可透過線上票券販售商以一鍵點擊滑鼠方式給予同意，須在營業時間撥打電話才可撤回同意，較為麻煩。

The requirement of an easy withdrawal is described as a necessary aspect of valid consent in the GDPR. If the withdrawal right does not meet the GDPR requirements, then the consent mechanism of the controller does not comply with the GDPR. As mentioned in section 3.1 on the condition of *informed* consent, the controller must inform the data subject of the right to withdraw consent prior to actually giving consent, pursuant to Article 7(3) of the GDPR. Additionally, the controller must as part of the transparency obligation inform the data subjects on how to exercise their rights.[52]
GDPR將簡易撤回的規範定性為有效同意的必要部分。若撤回權利未達到GDPR之要求，控管者的同意機制即不符合GDPR規範。如同在第3.1段關於*知情*同意之條件所述，按照GDPR第7條第3項規定，控管者應在當事人給予同意之前即告知其有撤回同意之權利。此外，控管者基於透明化義務，應告知當事人該如何行使權利[52]。

As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller.[53]
基於一般法理並依GDPR規定，同意經撤回後，所有依據同意而為的資料運用行為以及在撤回前已發生的同意均仍屬合法，然而，控管者應即終止該運用動作。若無其他合法基礎合法化資料運用行為（例如繼續儲存），控管者應將資料刪除[53]。

As mentioned earlier in these guidelines, it is very important that controllers assess the purposes for which data is actually processed and the lawful grounds on which it is based prior to collecting the data. Often companies need personal data for several purposes, and the processing is based on more than one lawful basis, e.g. customer data may be based on contract and consent. Hence, a withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the data subject. Controllers should therefore

[52] Recital 39 GDPR, which refers to Articles 13 and 14 of that Regulation, states that "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.
討論本規則第13條及第14條的GDPR前言第39點謂「自然人應受告知有關個人資料運用之風險、規則、安全維護及權利，以及如何行使與該運用行為有關之權利」。

[53] See Article 17(1)(b) and (3) GDPR.
見GDPR第17條第1項第b款及第3項。

be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon.
本指引前已提及，控管者在蒐集資料之前即評估運用資料之目的及所依據的合法事由一事至為重要。公司經常基於數個目的需要個人資料，並依不只一種合法基礎而運用，例如基於契約和同意而運用顧客資料。因此，撤回同意並不表示控管者須要刪除基於履行與當事人間的契約之目的而運用的資料。控管者應自始清楚掌握適用於各個資料之目的以及其合法基礎。

Controllers have an obligation to delete data that was processed on the basis of consent once that consent is withdrawn, assuming that there is no other purpose justifying the continued retention.[54] Besides this situation, covered in Article 17 (1)(b), an individual data subject may request erasure of other data concerning him that is processed on another lawful basis, e.g. on the basis of Article 6(1)(b).[55] Controllers are obliged to assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject.[56]
假如沒有其他目的可合法化持續保存行為時，控管者有義務在同意經撤回後即刪除基於同意而運用之資料[54]。除此情形之外，依第17條第1項第b款內容，個別當事人可請求刪除基於另一個合法基礎而運用的與其有關之其他資料，例如依據第6條第1項第b款[55]。即便當事人未請求刪除，控管者仍有義務評估繼續運用系爭資料是否適當[56]。

In cases where the data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate from consent (which is withdrawn) to this other lawful basis. Any change in the lawful basis for processing must be notified to a data subject in accordance with the information requirements in Articles 13 and 14 and under the general principle of transparency.
如當事人撤回同意而控管者仍欲以另一個合法基礎繼續運用個人資料時，控管者不可私下將同意（已被撤回）移轉至其他合法基礎。任何運用行為合法基礎的變更均應依照第13條及第14條對於資訊揭露的規範以及透明化的通常原則來通知當事人。

### 6. Interaction between consent and other lawful grounds in Article 6 GDPR
### 同意與GDPR第6條其他合法基礎的適用關係

Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose.[57]
第6條規定合法運用個資的要件，並設有6種控管者可依據的合法基礎。此6種合法基礎的適用必須在運用行為之前即已存在，且應與特定目的具備關聯性[57]。

It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an

[54] In that case, the other purpose justifying the processing must have its own separate legal basis. This does not mean the controller can swap from consent to another lawful basis, see section 6 below.
在此情形，其他可合法化運用行為之目的必須自行具備個別的法律基礎。這不表示控管者可任意由同意變更至另一個合法基礎，見下方第6部分。

[55] See Article 17, including exceptions that may apply, and Recital 65 GDPR
見第17條，包含可適用的例外，以及GDPR前言第65點

[56] See also Article 5 (1)(e) GDPR
見GDPR第5條第1項第e款

[57] Pursuant to Articles 13 (1)(c) and/or 14(1)(c), the controller must inform the data subject thereof.
依第13條第1項第c款及/或第14條第1項第c款規定，控管者應將此告知當事人。

individual withdraws consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals.
在此有必要說明，如控管者選擇以同意作為任何一部分運用的依據，即應重視該選擇，並對當事人撤回同意後即終止該部分之運用有所準備。如對外表示依據同意而運用資料，但實際上卻是依據其他的合法基礎時，將對個別當事人構成本質上的不公平。

In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.
換句話說，控管者不可將同意與其他合法基礎互換。舉例而言，當同意的有效性遇到問題時，不允許為了合法化運用行為而溯及適用正當利益作為依據。基於在蒐集個資的當下即應揭露控管者依據的合法基礎之規範，控管者應於蒐集之前即決定適用的合法依據。

## 7. Specific areas of concern in the GDPR
## GDPR中的特定領域考量

### 7.1. Children (Article 8)
### 兒童（第8條）

Compared to the current directive, the GDPR creates an additional layer of protection where personal data of vulnerable natural persons, especially children, are processed. Article 8 introduces additional obligations to ensure an enhanced level of data protection of children in relation to information society services. The reasons for the enhanced protection are specified in Recital 38: *" [...] they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data [...]"* Recital 38 also states that "*Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."* The words 'in particular' indicate that the specific protection is not confined to marketing or profiling but includes the wider 'collection of personal data with regard to children'.
相較於現行(95/46/EC)指令，GDPR針對特別是兒童等弱勢自然人的個資運用創設額外的保護層級。第8條對於資訊社會服務提出額外的義務，以確保強化兒童資料保護的等級。強化保護的理由載明於前言第38點：「*...他們對於風險、結果、有關的安全措施以及他們享有關於個資運用之權利等，可能較缺乏認知...*」。前言第38點也說明「*這類特定保護措施應尤其適用在基於行銷、建立人格或使用者檔案等目的而對兒童個人資料的利用行為，以及在使用直接對兒童提供之服務時，對兒童個人資料的蒐集行為*」。「尤其」一詞表示該特定保護措施並不限於行銷或建檔，尚包含更廣泛的「對兒童個人資料的蒐集行為」。

Article 8(1) states that where consent applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility

over the child.[58] Regarding the age limit of valid consent the GDPR provides flexibility, Member States can provide by law a lower age, but this age cannot be below 13 years.
第8條第1項表明，在直接向兒童提供資訊社會服務的情形，如適用同意時，該兒童須至少年滿16歲，運用該兒童的個人資料才屬合法。當該兒童未滿16歲時，該運用僅在兒童的法定代理人給予或授權之同意範圍內始屬合法[58]。GDPR對於有效同意的年齡限制提供彈性，成員國可以法律制定較低的年齡門檻，但不得低於13歲。

As mentioned in section 3.1. on informed consent, the information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children. In order to obtain "informed consent" from a child, the controller must explain in language that is clear and plain for children how it intends to process the data it collects.[59] If it is the parent that is supposed to consent, then a set of information may be required that allows adults to make an informed decision.
如同第3.1節關於知情同意所述，控管者對受眾提供的資訊應可得理解，且應特別考量兒童的立場。為了向兒童獲得「知情同意」，控管者必須使用對兒童來說清楚而簡白的語言，解釋將如何運用所蒐集的資料[59]。如果是應由家長同意的情形，可能便需要提供能讓成年人做出知情決定的一連串資訊。

It is clear from the foregoing that Article 8 shall only apply when the following conditions are met:
- The processing is related to the offer of information society services directly to a child.[60,61]
- The processing is based on consent.

由前述內容可知，第8條僅在滿足下列條件時始有適用：
- 該運用與直接向兒童提供資訊社會服務有關[60, 61]。
- 該運用是以同意為依據。

#### 7.1.1. Information society service
#### 資訊社會服務

To determine the scope of the term 'information society service" in the GDPR, reference is made in Article 4(25) GDPR to Directive 2015/1535.

[58] Without prejudice to the possibility of Member State law to derogate from the age limit, see Article 8(1).
無礙於成員國以法律降低年齡限制，見第8條第1項。

[59] Recital 58 GDPR re-affirms this obligation, in stating that, where appropriate, a controller should make sure the information provided is understandable for children.
GDPR前言第58點重申此義務，謂在適當時，控管者應確保提供予兒童的資訊可得理解。

[60] According to Article 4(25) GDPR an information society service means a service as defined in point (b) of Article 1(1) of Directive 2015/1535: "(b) 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request." An indicative list of services not covered by this definition is set out in Annex I of the said Directive. See also Recital 18 of Directive 2000/31.
根據GDPR第4條第25款規定，資訊社會服務依第2015/1535號指令第1條第1項第b款定義為：「(b)『服務』指任何資訊社會服務，也就是任何通常以電子方式提供的遠距而有償之服務，且屬於依接受服務者個別請求而提供之服務。為此定義之目的：(i)『遠距』意指提供該服務無須雙方同時在場；(ii)『以電子方式』意指該服務藉由電子設備發送及接受以運用（包含數位壓縮）並儲存資料，且完全透過有線、無線、光學方法或其他電磁方法而傳輸、傳達與接收；(iii)『依接受服務者個別請求』意指該服務係藉由傳輸資料之個別請求而提供」。該指令將不包含於此定義之服務列於附件1。亦見第2000/31號指令前言第18點。

[61] According to the UN Convention on the Protection of the Child, Article 1, "[…] a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier," see United Nations, General Assembly Resolution 44/25 of 20 November 1989 (Convention on the Rights of the Child).
根據聯合國兒童權利公約第1條，「[…]兒童係指未滿18歲之人，但該兒童適用之法律有較早成年之規定者從其規定」見聯合國1989年11月20日第44/25號大會決議（兒童權利公約）。

為了決定GDPR所稱「資訊社會服務」的範圍，GDPR第4條第25款即規定應參照適用2015/1535指令。

While assessing the scope of this definition, WP29 also refers to case law of the ECJ.[62] The ECJ held that *information society services* cover contracts and other services that are concluded or transmitted on-line. Where a service has two economically independent components, one being the online component, such as the offer and the acceptance of an offer in the context of the conclusion of a contract or the information relating to products or services, including marketing activities, this component is defined as an information society service, the other component being the physical delivery or distribution of goods is not covered by the notion of an information society service. The online delivery of a service would fall within the scope of the term *information society service* in Article 8 GDPR.

在評估此定義的範圍時，WP29條同時參考歐洲法院的判例法[62]。歐洲法院認為，*資訊社會服務*包含在線上締結或傳送的契約和其他服務。當某服務包含兩個經濟上獨立的要素，其一是線上要素，例如為締結契約所為的要約與承諾行為，或是提供與產品或服務有關之資訊，包含行銷活動，此要素即定義為資訊社會服務。另一要素為實體的商品寄送或銷售，則不包含在資訊社會服務的概念中。線上提供的服務則涵蓋於GDPR第8條所稱*資訊社會服務*的範圍。

#### 7.1.2. Offered directly to a child
#### 直接對兒童提供

The inclusion of the wording 'offered directly to a child' indicates that Article 8 is intended to apply to some, not all information society services. In this respect, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply.

條文中包含「直接對兒童提供」，代表第8條僅欲適用於某些資訊社會服務。就此而言，如果資訊社會服務提供者清楚向潛在使用者表示其僅提供服務予18歲以上之人，且無其他證據（例如網站內容或行銷計畫）顯示相反情形，則該服務將不被認為是「直接對兒童提供」，第8條即不適用。

#### 7.1.3. Age
#### 年齡

The GDPR specifies that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."* The controller must be aware of those different national laws, by taking into account the public targeted by its services. In particular it should be noted that a controller providing a cross-border service cannot always rely on complying with only the law of the Member State in which it has its main establishment but may need to

[62] See European Court of Justice, 2 December 2010 Case C-108/09, (Ker-Optika), paragraphs 22 and 28. In relation to 'composite services', WP29 also refers to Case C-434/15 (AsociacionProfesional Elite Taxi v Uber Systems Spain SL), para 40, which states that an information society service forming an integral part of an overall service whose main component is not an information society service (in this case a transport service), must not be qualified as 'an information society service'.
見歐洲法院2010年12月2號C-108/09判決，（Ker-Optika），第22段及第28段。關於「綜合服務」部分，WP29亦參考C-434/15 (Asociacion Profesional Elite Taxi v Uber Systems Spain SL)判決，第40段，該段謂若一項資訊社會服務是某完整服務的一部分，但該完整服務的主要內容並非資訊社會服務（本案即指交通運輸服務）時，即不滿足「資訊社會服務」之要件。

comply with the respective national laws of each Member State in which it offers the information society service(s). This depends on whether a Member State chooses to use the place of main establishment of the controller as a point of reference in its national law, or the residence of the data subject. First of all the Member States shall consider the best interests of the child during making their choice. The Working Group encourages the Member States to search for a harmonized solution in this matter.
GDPR明確指出「*成員國可以法律為該目的訂定較低的年齡限制，但不可低於13歲*」。控管者應考量其服務鎖定之對象而留意不同國家的法律。應特別說明的是，提供跨境服務的控管者無法僅遵守其主要據點所在地的國家法律，而可能需要遵守其提供資訊社會服務所及的各個國家的各別法律。這取決於該成員國選擇以控管者的主要營業據點所在地或當事人的居住地作為適用內國法律的判斷依據。成員國在選擇時，首要考慮兒童的最佳利益。工作組鼓勵成員國就此議題尋找調和的解決方案。

When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities.
在以同意為依據而對兒童提供資訊社會服務時，控管者被期待採取合理的努力去驗證以電子方式同意的使用者已超過年齡標準，且這些措施與運用行為的性質與風險間應符合比例原則。

If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.
如使用者聲稱已超過電子方式同意的年齡，控管者即可以適當查驗方式驗證該聲明是否真實。雖然GDPR並未明確要求須採取合理的努力以驗證年齡，但仍隱含寓有此意，因為如果未達到能自行提供有效同意之年齡標準的兒童給予同意時，將導致資料運用違反法律。

If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility.
如使用者聲稱未達到電子方式同意的年齡，控管者可無須進一步查驗而接受該聲明，但將需要再獲得家長授權，且須驗證提供該同意之人為法定代理人。

Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor.[63] If doubts arise the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required.[64]
驗證年齡不應導致過度的資料運用。驗證當事人年齡的機制應包含對運用行為的風險評估。

[63] Although this may not be a watertight solution in all cases, it is an example to deal with this provision
雖然這可能不是最嚴謹的解決方案，但不失為因應本條規範的示例
[64] See WP29 Opinion 5/2009 on social networking services (WP 163).
見WP29意見5/2009關於社會網路服務（WP163）。

在某些低風險情形，要求服務的新訂戶揭露其出生年份或填寫表格聲明「非」未成年人，可能是適當的[63]。如有疑慮時，控管者應在具體個案審查其年齡驗證機制，並考慮是否需要替代的查驗方式[64]。

### 7.1.4. Children's consent and parental responsibility
### 兒童同意與法定代理權

Regarding the authorisation of a holder of parental responsibility, the GDPR does not specify practical ways to gather the parent's consent or to establish that someone is entitled to perform this action.[65] Therefore, the WP29 recommends the adoption of a proportionate approach, in line with Article 8(2) GDPR and Article 5(1)(c) GDPR (data minimisation). A proportionate approach may be to focus on obtaining a limited amount of information, such as contact details of a parent or guardian.

對於法定代理人的授權，GDPR並未明確規定取得父母同意或建立有權行使該行為的實務作法[65]。因此，WP29建議依照GDPR第8條第2項及第5條第1項第c款（資料最小化）之意，採取符合比例原則的方法為之。符合比例原則的方法或許可著重於僅取得有限的資訊，例如父母或監護人的聯絡方式。

What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR.[66] Trusted third party verification services may offer solutions which minimise the amount of personal data the controller has to process itself.

對於「使用者的年齡已足夠自行提供同意」與「代表兒童提供同意之人確實為法定代理人」之驗證方式是否合理，可能取決於運用造成的風險以及可得的技術而定。在低風險案例，以電子郵件驗證法定代理權可能即已足夠。相對地，在高風險案例，要求更多的證據可能較為妥當，這樣控管者才可驗證並依GDPR第7條第1項規定保存資訊[66]。受信任之第三方驗證服務或可提供解決方案，最少化控管者須自行運用的個人資料。

> [Example 23] An online gaming platform wants to make sure underage customers only subscribe to its services with the consent of their parents or guardians. The controller follows these steps:
> Step 1: ask the user to state whether they are under or over the age of 16 (or alternative age of digital consent)
> If the user states that they are under the age of digital consent:
> Step 2: service informs the child that a parent or guardian needs to consent or authorise the processing before the service is provided to the child. The user is requested to disclose the email address of a parent or guardian.
> Step 3: service contacts the parent or guardian and obtains their consent via email for processing and take reasonable steps to confirm that the adult has parental responsibility.

[65] WP 29 notes that it not always the case that the holder of parental responsibility is the natural parent of the child and that parental responsibility can be held by multiple parties which may include legal as well as natural persons.
WP29指出，並非所有法定代理人均為該兒童的原生父母，且該法定代理權可由包含法人與自然人在內的多方共同行使。

[66] For example, a parent or guardian could be asked to make a payment of €0,01 to the controller via a bank transaction, including a brief confirmation in the description line of the transaction that the bank account holder is a holder of parental responsibility over the user. Where appropriate, an alternative method of verification should be provided to prevent undue discriminatory treatment of persons that do not have a bank account.
例如可要求父母或監護人透過銀行交易給付控管者0.01歐元，並在交易的描述列記載該銀行帳戶持有人為該使用者之法定代理人的簡要確認聲明。如適當時，應向未持有銀行帳戶之人提供驗證身分的替代方案，以避免不當的差別待遇。

Step 4: in case of complaints, the platform takes additional steps to verify the age of the subscriber.
If the platform has met the other consent requirements, the platform can comply with the additional criteria of Article 8 GDPR by following these steps.

[示例23]某線上遊戲平台要確保未達年齡限制的客戶僅在父母或監護人同意的情形下訂購服務。該控管者遵循下列步驟：

步驟1：要求使用者聲明是否低於或高於16歲（或以電子方式同意的其他年齡限制）。如使用者聲稱未達使用電子方式同意的年齡：

步驟2：該服務提醒兒童，在向其提供服務之前，需要有父母或監護人的同意或授權。該使用者被要求提供一位父母或監護人的電子郵件信箱。

步驟3：該服務與該父母或監護人聯繫，並透過電子郵件取得其對運用的同意，且以合理步驟確認該成年人是法定代理人。

步驟4：如有申訴情形，該平台即採取額外步驟驗證訂戶的年齡。

如該平台滿足同意的其他規範，即可依循上述步驟遵守GDPR第8條的額外標準。

The example shows that the controller can put itself in a position to show that reasonable efforts have been made to ensure that valid consent has been obtained, in relation to the services provided to a child. Article 8(2) particularly adds that "*The controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*"

此示例顯示，控管者在向兒童提供服務時，證明自己已做出合理的努力以確保獲得之同意為有效。第8條第2項特別加入「*控管者應做出合理的努力，考量在既有技術的情況下，驗證同意是由該兒童的法定代理人給予或授權*」。

It is up to the controller to determine what measures are appropriate in a specific case. As a general rule, controllers should avoid verification solutions which themselves involve excessive collection of personal data.

控管者可自行決定特定個案中的適當方式。原則上，控管者應避免需要過度蒐集個人資料的驗證方案。

WP29 acknowledges that there may be cases where verification is challenging (for example where children providing their own consent have not yet established an 'identity footprint', or where parental responsibility is not easily checked. This can be taken into account when deciding what efforts are reasonable, but controllers will also be expected to keep their processes and the available technology under constant review.

WP29瞭解有些情形可能難以執行驗證（例如尚未建立「身分足跡」而自行提供同意的兒童，或無法輕易查驗法定代理權的情形。在決定何種努力屬於合理時，可將這類情形納入考量，但控管者也被期待持續檢視其運用行為與可得技術。

With regard to the data subject's autonomy to consent to the processing of their personal data and have full control over the processing, consent by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data of children can be confirmed, modified or withdrawn, once the data subject reaches the age of digital consent.

In practice, this means that if the child does not take any action, consent given by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data given prior to the age of digital consent, will remain a valid ground for processing.

After reaching the age of digital consent, the child will have the possibility to withdraw the consent himself, in line with Article 7(3). In accordance with the principles of fairness and accountability, the controller must inform the child about this possibility.[67]
在當事人同意運用其個人資料的自主性以及對於運用的完整控制方面，原本由法定代理人對運用兒童的個人資料所為之同意或授權，當事人一旦達到電子方式同意的年齡門檻後，即可確認、修改或撤回。
實務上，這表示如該兒童並未採取任何行動，則在達到電子方式同意的年齡限制之前已由法定代理人對運用兒童的個人資料所為之同意或授權，仍將成為運用的有效依據。
在達到電子方式同意的年齡門檻後，該兒童將有可能依第7條第3項撤回同意。基於公平性與課責性原則，控管者應告知該兒童有關撤回同意的選擇[67]。

It is important to point out that in accordance with Recital 38, consent by a parent or guardian is not required in the context of preventive or counselling services offered directly to a child. For example the provision of child protection services offered online to a child by means of an online chat service do not require prior parental authorisation.
在此有必要指出，依照前言第38點規定，直接對兒童提供的預防性或諮詢性服務即不需要父母或監護人的同意。舉例來說，藉由線上對話服務的方式，在線上對兒童提供保護的服務便不需要家長事前授權。

Finally, the GDPR states that the rules concerning parental authorization requirements vis-à-vis minors shall not interfere with "the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child". Therefore, the requirements for valid consent for the use of data about children are part of a legal framework that must be regarded as separate from national contract law. Therefore, this guidance paper does not deal with the question whether it is lawful for a minor to conclude online contracts. Both legal regimes may apply simultaneously, and, the scope of the GDPR does not include harmonization of national provisions of contract law.
最後，GDPR強調，有關未成年人的家長授權之規定不應妨礙「成員國之一般契約法，例如關於兒童之契約效力、形式或效果」。因此，獲得有效同意以利用兒童資料的規範係法律框架的一部分，須與內國契約法律區分視之。故本指引文件並不處理未成年人締結線上契約是否合法的問題。兩種法律制度可能同時適用，且GDPR的範圍並不包含調和各國的契約法律規範。

### 7.2. Scientific research
### 科學研究

The definition of scientific research purposes has substantial ramifications for the range of data processing activities a controller may undertake. The term *'scientific research'* is not defined in the GDPR. Recital 159 states "(…) *For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner.* (…)", however the WP29 considers the notion may not be stretched beyond its common meaning and understands that '*scientific research'* in this context means a research project set up in accordance with relevant

[67] Also, data subjects should be aware of the right to be forgotten as laid down in Article 17, which is in particular relevant for consent given when the data subject was still a child, see recital 63.
同時，當事人應獲知第17條規定的被遺忘權，此在給予同意的當事人仍為兒童時尤其重要，見前言第63點。

sector-related methodological and ethical standards, in conformity with good practice.
科學研究目的之定義對於控管者可從事的資料運用行為之範圍具有重大影響。GDPR並未定義「*科學研究*」一詞。前言第159點謂「（...）*基於本規則之目的，應以寬鬆方式解釋為科學研究目的而運用個人資料*。（...）」然而WP29認為不應將其概念延伸至通常意義之外，並瞭解在此脈絡下的「*科學研究*」意指符合相關領域之方法論及倫理標準，且遵循優良實務的研究計畫。

When consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation. An example of such a procedural obligation, where the processing is based not on consent but on another legal basis, is to be found in the Clinical Trials Regulation. In the context of data protection law, the latter form of consent could be considered as an additional safeguard.[68] At the same time, the GDPR does not restrict the application of Article 6 to consent alone, with regard to processing data for research purposes. As long as appropriate safeguards are in place, such as the requirements under Article 89(1), and the processing is fair, lawful, transparent and accords with data minimisation standards and individual rights, other lawful bases such as Article 6(1)(e) or (f) may be available.[69] This also applies to special categories of data pursuant to the derogation of Article 9(2)(j).[70]
當依照GDPR規定而以同意作為進行研究的法律依據時，針對使用個人資料的同意應與其他針對倫理標準或程序義務所需要的同意有所區別。在臨床試驗規則中即可找到程序義務的示例，此時運用行為並非以同意為依據而是其他的法律基礎。在資料保護法律的背景下，後者形式的同意可視為一種額外的安全措施[68]。在此同時，GDPR並未限制適用第6條規定僅以同意作為基於研究目的而運用資料之依據。只要存有適當安全維護，例如第89條第1項的規範，且該運用具備公平性、合法性、透明化，並與資料最小化標準與個人之權利具備一致性，其他例如第6條第1項第e款或第f款的合法依據也可能適用[69]。此亦適用於第9條第2項第j款對特種個資所設之例外條款[70]。

Recital 33 seems to bring some flexibility to the degree of specification and granularity of consent in the context of scientific research. Recital 33 states: "*It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose*."
前言第33點對於科學研究中的同意之特定性與區別性提供些許彈性。前言第33點謂：「*通常不太可能在資料蒐集時便完整識別為科學研究而運用個人資料之目的。因此，如符合科學研究公認的倫理標準時，應允許當事人僅就特定範圍的科學研究給予同意。當事人應有機會僅對特定研究範圍或預期目的允許範圍內的部分研究計畫給予同意*」。

[68] See also Recital 161 of the GDPR.
見GDPR前言第161點。
[69] Article 6(1)(c) may also be applicable for parts of the processing operations specifically required by law, such as gathering reliable and robust data following the protocol as approved by the Member State under the Clinical Trial Regulation.
第6條第1項第c款也可適用於法律特別要求的部分運用行為，例如在臨床試驗規則下，遵守成員國許可的計畫而蒐集可信賴及可靠之資料。
[70] Specific testing of medicinal products may take place on the basis of an EU or national law pursuant to Article 9(2)(i).
依第9條第2項第i款規定，可基於歐盟或國家法律的規定而對藥品為特定測試。

First, it should be noted that Recital 33 does not disapply the obligations with regard to the requirement of specific consent. This means that, in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level.
首應說明的是，前言第33點非謂無須適用關於特定同意之規範的義務。其意指原則上僅在詳實描述目的之前提下，科學研究計畫才可以同意為依據而將個人資料包含在內。在一開始無法明確指出科學研究計畫所涉及資料運用目的之情形，前言第33點例外允許以較籠統的程度描述該目的。

Considering the strict conditions stated by Article 9 GDPR regarding the processing of special categories of data, WP29 notes that when special categories of data are processed on the basis of explicit consent, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny.
考量到GDPR第9條關於運用特種個資的嚴格條件，WP29指出，在以明確同意為依據而運用特種個資的情況，當適用前言第33點所述較有彈性的方法時，應採取較嚴格的解釋，且需要高強度的監督。

When regarded as a whole, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked.
整體而言，GDPR不允許控管者規避向當事人指明目的以取得同意之重要原則。

When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research.
當無法完整指明研究目的時，控管者應尋求其他方式以確保最大程度滿足同意的規範意旨，例如允許當事人以較概略方式同意研究目的，以及同意一開始即知的研究計畫之特定階段。隨著研究的進展，便可在下一階段開始前獲得對該計畫後續步驟的同意。不過，該同意仍應符合科學研究適用的倫理標準。

Moreover, the controller may apply further safeguards in such cases. Article 89(1), for example, highlights the need for safeguards in data processing activities for scientific or historical or statistical purposes. These purposes "*shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of data subject*." Data minimization, anonymisation and data security are mentioned as possible safeguards.[71] Anonymisation is the preferred solution as

[71] See for example Recital 156. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials, see Recital 156, mentioning Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use. See also WP29 Opinion 15/2011 on the definition of consent (WP 187), p. 7: "Moreover, obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality.
For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose." […] As a principle, consent should not be seen as an exemption from the other data protection principles, but as a safeguard. It is primarily a ground for lawfulness, and it does not waive the application of other principles."
示例見前言第156點。為科學目的運用個人資料也應遵守其他相關法律，例如有關臨床試驗之法律，前言第156點提及歐洲議會

soon as the purpose of the research can be achieved without the processing of personal data.
除此之外，控管者在此類個案中可採取進一步的安全維護。舉例來說，第89條第1項強調在為科學、歷史或統計目的而運用資料行為中的安全維護需求。這些目的「*應依本規則規定而有適當的安全維護，以保障當事人的權利與自由*」。資料最小化、匿名化以及資料安全是被提及可能的安全維護措施[71]。一旦不再需要運用個人資料也能達成研究目的時，匿名化將是較佳的解決方案。

Transparency is an additional safeguard when the circumstances of the research do not allow for a specific consent. A lack of purpose specification may be offset by information on the development of the purpose being provided regularly by controllers as the research project progresses so that, over time, the consent will be as specific as possible. When doing so, the data subject has at least a basic understanding of the state of play, allowing him/her to assess whether or not to use, for example, the right to withdraw consent pursuant to Article 7(3).[72]
當該研究無法取得特定同意時，透明化即為一個額外的安全維護措施。目的特定性的不足可經由控管者在研究計畫進行中定期告知目的之最新發展資訊而補足，隨著時間經過，同意將將越來越明確。在過程中，當事人至少對現況能有基本的理解，以供其評估是否行使例如第7條第3項的撤回同意權[72]。

Also, having a comprehensive research plan available for data subjects to take note of, before they consent could help to compensate a lack of purpose specification.[73] This research plan should specify the research questions and working methods envisaged as clearly as possible. The research plan could also contribute to compliance with Article 7(1), as controllers need to show what information was available to data subjects at the time of consent in order to be able to demonstrate that consent is valid.
同時，在當事人同意之前便提供詳盡的研究計畫供其留意，亦可彌補目的特定性的不足[73]。該研究計畫應盡可能明確記載研究議題與預計的執行方法。此研究計劃亦有助於遵守第7條第1項規定，因為控管者必須能提出當事人在同意的當下取得哪些資訊，以便證明該同意之有效性。

It is important to recall that where consent is being used as the lawful basis for processing there must be a possibility for a data subject to withdraw that consent. WP29 notes that withdrawal of consent could undermine types scientific research that require data that can be linked to individuals, however the GDPR is clear that consent can be withdrawn and controllers must act upon this –there is no exemption to this requirement for scientific research. If a controller receives a withdrawal request, it must in principle delete the personal data straight away if it wishes to continue to use the data for the purposes of the research.[74]

---

與歐盟理事會2014年4月16日關於為人體使用藥物之臨床試驗的歐盟第536/2014號規則。亦見WP29 15/2011關於同意的定義之意見書（WP187），第7頁：「此外，取得同意並不免除控管者在第6條下有關公平性、必要性、合比例性，以及資料品質等義務。舉例來說，即便基於使用者同意而運用個資，亦無法合法化超出特定目的所為的資料蒐集。[…]原則上，不可將同意視為其他資料保護原則的豁免，而應視為一種安全維護。同意主要是一項合法基礎，並不免除其他原則的適用」。

[72] Other transparency measures may also be relevant. When controllers engage in data processing for scientific purposes, while full information cannot be provided at the outset, they could designate a specific contact person for data subjects to address with questions.
其他透明化措施也可能相關。當控管者基於科學目的而運用個資，但無法在一開始便提供完整資訊時，控管者可為當事人指派特定聯絡人以處理詢問。

[73] Such a possibility can be found in Article 14(1) of the current Personal Data Act of Finland (Henkilötietolaki, 523/1999)
在現行芬蘭個人資料保護法（Henkilötietolaki, 523/1999）第14條第1項可見相關適用。

[74] See also WP29 Opinion 05/2014 on "Anonymisation Techniques" (WP216).

在此有必要重申，當以同意作為運用的合法依據時，當事人必須能夠撤回同意。WP29指出，撤回同意可能會對需與個資相連結的科學研究類型有所損害，然而GDPR清楚規定同意可被撤回，而控管者的行為必須受其拘束，此規範對於科學研究並無例外。當控管者收到撤回請求時，即使其有意繼續基於研究目的而使用資料，原則上即應立刻刪除個人資料[74]。

### 7.3. Data subject's rights
### 當事人權利

If a data processing activity is based on a data subject's consent, this will affect that individual's rights. Data subjects may have the right to data portability (Article 20) when processing is based on consent. At the same time, the right to object (Article 21) does not apply when processing is based on consent, although the right to withdraw consent at any time may provide a similar outcome.
如某資料運用行為是以當事人之同意為依據，此將影響該當事人的權利。當運用是以同意為依據時，當事人享有個資可攜權（第20條）。同時，拒絕權（第21條）並不適用在以同意為依據而運用的情形，雖然可隨時撤回同意的權利可提供類似效果。

Articles 16 to 20 of the GDPR indicate that (when data processing is based on consent), data subjects have the right to erasure when consent has been withdrawn and the rights to restriction, rectification and access.[75]
GDPR第16條至第20條表明（當以同意作為運用資料之依據時），當事人有權在撤回同意後請求刪除資料，並有權限制、修改及近用資料[75]。

## 8. Consent obtained under Directive 95/46/EC
## 在95/46/EC指令下獲得之同意

Controllers that currently process data on the basis of consent in compliance with national data protection law are not automatically required to completely refresh all existing consent relations with data subjects in preparation for the GDPR. Consent which has been obtained to date continues to be valid in so far as it is in line with the conditions laid down in the GDPR.
對於目前遵守國家資料保護法律而以同意為運用資料之依據的控管者來說，並不需要因為因應GDPR而更新所有與當事人間現有的同意關係。只要與GDPR規定的條件相符，迄今已獲得的同意將持續有效。

It is important for controllers to review current work processes and records in detail, before 25 May 2018, to be sure existing consents meet the GDPR standard (see Recital 171 of the GDPR[76]). In practice, the GDPR raises the bar with regard to implementing consent mechanisms and introduces

---

見WP29 05/2014關於「匿名化技術」之意見書（WP216）。

[75] In cases where certain data processing activities are restricted in accordance with Article 18, GDPR, consent of the data subject may be needed to lift restrictions.
依GDPR第18條規定，在某些資料運用活動受到限制的情形下，解除限制可能需要當事人的同意。

[76] Recital 171 GDPR states: "Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed."
GDPR前言第171點謂：「本規則取代95/46/EC指令。在本規則施行日前已在進行的運用行為應於本規則生效後兩年內使其符合本規則規定。對於依95/46/EC指令規定以同意為依據的運用行為，如給予同意的方式與本規則規定之要件相符，當事人不必然需要再次給予同意，即可由控管者在本規則施行日後繼續該運用行為。執委會通過之決定及監管機關依95/46/EC指令所為之授權，於修正、取代或廢止前仍繼續有效」。

several new requirements that require controllers to alter consent mechanisms, rather than rewriting privacy policies alone.[77]
對控管者重要的是，在2018年5月25日前細部審查現行的工作流程與紀錄，以確保現有的同意達到GDPR的標準（見GDPR前言第171點[76]）。在實踐上，GDPR對建置同意機制提高標準，並增設數項新規以要求控管者修改同意機制，而非僅是重新撰寫隱私政策[77]。

For example, as the GDPR requires that a controller must be able to demonstrate that valid consent was obtained, all presumed consents of which no references are kept will automatically be below the consent standard of the GDPR and will need to be renewed. Likewise as the GDPR requires a "statement or a clear affirmative action", all presumed consents that were based on a more implied form of action by the data subject (e.g. a pre-ticked opt-in box) will also not be apt to the GDPR standard of consent.
舉例來說，由於GDPR要求控管者須可證明獲得有效同意，因此所有未保存參考資訊的推定同意將當然低於GDPR的同意標準，並需要更新。同樣地，因為GDPR要求「聲明或清楚肯定的行動」，因此所有基於當事人以較為暗示之行動（例如預先勾選的選擇同意框格）表達的推定同意，就GDPR的同意標準來說也不恰當。

Furthermore, to be able to demonstrate that consent was obtained or to allow for more granular indications of the data subject's wishes, operations and IT systems may need revision. Also, mechanisms for data subjects to withdraw their consent easily must be available and information about how to withdraw consent must be provided. If existing procedures for obtaining and managing consent do not meet the GDPR's standards, controllers will need to obtain fresh GDPR-compliant consent.
因此，為能證明獲得同意，或能允許更有區別地表達當事人的意思，作業和資訊系統可能需要改版。此外，讓當事人能輕易撤回同意之機制必須存在，且須提供如何撤回同意之資訊。如果現有之獲得與管理同意的程序不符合GDPR標準，控管者將需要獲得新的符合GDPR之同意。

On the other hand, as not all elements named in Articles 13 and 14 must always be present as a condition for informed consent, the extended information obligations under the GDPR do not necessarily oppose the continuity of consent which has been granted before the GDPR enters into force (see page 15 above). Under Directive 95/46/EC, there was no requirement to inform data subjects of the basis upon which the processing was being conducted.
另一方面，由於知情同意的條件並未要求揭露第13條或第14條的所有要素，GDPR擴增的資訊義務不必然影響在GDPR生效前即已給予之同意的持續有效性（見上方第15頁）（譯註：即本翻譯文件第21頁）。在95/46/EC指令下，並無規範要求將運用之法律依據告知當事人。

If a controller finds that the consent previously obtained under the old legislation will not meet the standard of GDPR consent, then controllers must undertake action to comply with these standards, for example by refreshing consent in a GDPR-compliant way. Under the GDPR, it is not possible to swap between one lawful basis and another. If a controller is unable to renew consent in a compliant way and is also unable –as a one off situation- to make the transition to GDPR compliance by basing data processing on a different lawful basis while ensuring that continued processing is fair

[77] As indicated in the introduction, the GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. Many of the new requirements build upon Opinion 15/2011 on consent.
如導言所述，GDPR對於「取得及舉證有效同意」提出更清楚與詳盡的規範。許多新規定是以15/2011關於同意之意見書為依據。

and accounted for, the processing activities must be stopped. In any event the controller needs to observe the principles of lawful, fair and transparent processing.

如控管者發現，之前在舊法下獲得的同意無法符合GDPR的同意標準時，控管者即應採取行動以遵循該標準，例如以符合GDPR的方式更新同意。在GDPR下，不得在不同合法基礎之間任意變換。如控管者無法以合規方式更新同意，也無法一次性地以不同的資料運用合法基礎轉換至符合GDPR規範，並能同時確保繼續運用符合公平性與課責性時，即應終止該運用行為。在任何情況下，控管者都需要注意合法、公平與透明運用之原則。

**-*-*-*-*-*-*-*-*-*-*-*-* END OF DOCUMENT *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-***