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

17/EN
WP251rev.01

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679
關於第 2016/679 號規則(GDPR)中的自動化個人決策和剖析之指引

Adopted on 3 October 2017

2017 年 10 月 3 日通過

As last Revised and Adopted on 6 February 2018

2018 年 2 月 6 日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and 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/justice/data-protection/index_en.htm
網址：http://ec.europa.eu/justice/data-protection/index_en.htm

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,

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，

having regard to Articles 29 and 30 thereof,

基於該指令第29條及第30條，

having regard to its Rules of Procedure,

基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:

通過此份指引：

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

TABLE OF CONTENTS 目錄

I. Introduction
導言

The General Data Protection Regulation (the GDPR), specifically addresses profiling and automated individual decision-making, including profiling.[1]

一般資料保護規則（GDPR）特別規範剖析和自動化個人決策（包含剖析）。[1]

Profiling and automated decision-making are used in an increasing number of sectors, both private and public. Banking and finance, healthcare, taxation, insurance, marketing and advertising are just a few examples of the fields where profiling is being carried out more regularly to aid decision-making.

使用剖析和自動化決策之產業逐漸增加，包含私人或公共部門。銀行和金融、醫療保健、稅務、保險、行銷和廣告僅是幾個經常使用剖析協助決策之行業示例。

Advances in technology and the capabilities of big data analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms.

技術的進步以及大數據分析、人工智慧和機器學習的能力使得剖析建檔和做出自動化決策變得更加容易，且有對於個人的權利和自由產生重大影響之可能。

The widespread availability of personal data on the internet and from Internet of Things (IoT) devices, and the ability to find correlations and create links, can allow aspects of an individual's

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, an d repealing Directive 95/46/EC. Profiling and automated individual decision-making are also covered by Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. While these guidelines focus on profiling and automated individual decision-making under the GDPR, the guidance is also relevant regarding the two topics under Directive 2016/680, with respect to their similar provisions. The analysis of specific features of profiling and automated individual decision-making under Directive 2016/680 is not included in these guidelines, since guidance in this respect is provided by the Opinion WP258 "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", adopted by WP29 on 29 November 2017 This Opinion covers automated individual decision - making and profiling in the context of law enforcement data processing at pages 11-14 and is available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178
2016年4月27日歐洲議會和歐盟理事會在個人資料運用上為保護自然人與確保該資料之自由流通，制定第2016/679號規則(EU)，並廢除第95/46 / EC號指令。2016年4月27日歐洲議會和理事會第2016/680號指令(EU)亦涵蓋了剖析和自動化個人決策，關於權責機關為預防、調查、偵查或起訴刑事犯罪或執行刑事處罰而運用個人資料時，對自然人之保護與確保該資料之自由流通。雖然本指引著重於GDPR下之剖析和自動化個人決策，但本指導與第2016/680號指令中就此兩項主題之類似規定亦為相關。第2016/680號指令中之剖析和自動化個人決策的具體特徵分析並未涵蓋於本指引中，因WP258意見「關於執法指令之關鍵議題意見」(EU 2016/680)提供了此方面之指導，WP29於2017年11月29日通過。此意見第11-14頁涵蓋了執法資料運用背景下之自動化個人決策和剖析，請參閱：
http：//ec.europa.eu/newsroom/article29/item-detail.cfm？ITEM_ID=610178

personality or behaviour, interests and habits to be determined, analysed and predicted.
網路和物聯網（IoT）設備上個人資料之廣泛可得性以及發現關聯性和建立連結之能力，使得當事人之個性或行為、興趣和習慣等各個面向皆可被確認、分析和預測。

Profiling and automated decision-making can be useful for individuals and organisations, delivering benefits such as:
剖析和自動化決策對個人及組織是有幫助的，其可帶來之益處如：

- increased efficiencies; and
  提高效率；及
- resource savings.
  節省資源。

They have many commercial applications, for example, they can be used to better segment markets and tailor services and products to align with individual needs. Medicine, education, healthcare and transportation can also all benefit from these processes.
剖析和自動化決策具有許多商業應用，例如，可用以妥善劃分市場、訂製服務及符合個人化需求之產品。醫學、教育、醫療保健和交通運輸亦受益於這些運用。

However, profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards.
然而，剖析和自動化決策可能會對需要適當安全維護措施之個人權利和自由造成重大風險。

These processes can be opaque. Individuals might not know that they are being profiled or understand what is involved.
這些運用可能是不透明的。個人可能無法得知正在被剖析或理解其所涉及之內容。

Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustified discrimination.
剖析可能將現有的刻板印象和社會隔離永久化。剖析亦可能將某個人鎖定於特定類型，並將其限於被建議之偏好。此亦會損害其選擇某些產品或服務（如書籍、音樂或新聞來源）之自由。在某些情況下，剖析可能會造成預測之不準確。而於其他情況中，剖析可能造成拒絕提供服務和產品以及不合理歧視。

The GDPR introduces new provisions to address the risks arising from profiling and automated

decision-making, notably, but not limited to, privacy. The purpose of these guidelines is to clarify those provisions.
GDPR引進了新的規定以因應剖析和自動化決策所帶來之風險，尤其是隱私權(但不以此為限)。本指引之目的即是在闡明這些規定。

This document covers:
本文件涵蓋：

- Definitions of profiling and automated decision-making and the GDPR approach to these in general – Chapter II
  剖析和自動化決策之定義以及GDPR對此之總體態度 - 第二章
- General provisions on profiling and automated decision-making – Chapter III
  剖析和自動化決策之一般規定 - 第三章
- Specific provisions on solely automated decision-making defined in Article 22 - Chapter IV
  第22條定義之純自動化決策具體規定- 第四章
- Children and profiling – Chapter V
  兒童和剖析 - 第五章
- Data protection impact assessments and data protection officers– Chapter VI
  個資保護影響評估和個資保護長 - 第六章

The Annexes provide best practice recommendations, building on the experience gained in EU Member States.
附錄依據歐盟成員國之經驗提供最佳實務作法建議。

The Article 29 Data Protection Working Party (WP29) will monitor the implementation of these guidelines and may complement them with further details as appropriate.
第29條個資保護工作小組（WP29）將監督本指引之執行情況，並可酌情補充進一步細節。

II. Definitions
定義

The GDPR introduces provisions to ensure that profiling and automated individual decision-making (whether or not this includes profiling) are not used in ways that have an unjustified impact on individuals' rights; for example:
GDPR引進了某些規定以確保剖析和自動化個人決策（無論是否包含剖析）之使用方式不

會對個人權利產生不合理之影響; 例如：

- specific transparency and fairness requirements;
  具體透明和公正性之要求；
- greater accountability obligations;
  更高之課責義務；
- specified legal bases for the processing;
  運用之具體法律基礎；
- rights for individuals to oppose profiling and specifically profiling for marketing; and
  當事人拒絕剖析和專為行銷目的之剖析的權利；及
- if certain conditions are met, the need to carry out a data protection impact assessment.
  若滿足某些要件，則需辦理個資保護影響評估。

The GDPR does not just focus on the decisions made as a result of automated processing or profiling. It applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals.
GDPR並非只著重自動運用或剖析結果所為之決策。GDPR適用於為建立剖析檔案而蒐集之資料，以及這些剖析對當事人之應用。

A. Profiling
剖析

The GDPR defines profiling in Article 4(4) as:
GDPR於第4條第4款將剖析定義為：

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
> 任何形式之個人資料自動化運用，包含使用個人資料評估與自然人相關之某些個人面向，尤其是分析或預測有關該自然人在工作上之表現、經濟狀況、健康、個人偏好、興趣 、可信度、行為、所在位置或移動；

Profiling is composed of three elements:

剖析由三項要件組成：

- it has to be an *automated* form of processing;
  剖析必須是一種*自動化*的運用形式；
- it has to be carried out *on personal data*; and
  剖析必須是*針對個人資料*之執行；及
- the objective of the profiling must be *to evaluate personal aspects* about a natural person.
  剖析之目的必須是*評估*關於自然人之*個人面向*。

Article 4(4) refers to 'any form of automated processing' rather than 'solely' automated processing (referred to in Article 22). Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition.
第4條第4款指的是「任何形式之自動化運用」而非「純」自動化之運用（請參閱第22條）。剖析必須涉及某種形式之自動化運用 – 即使人為參與並不一定會將活動排除於此定義之外。

Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.
剖析係一種可能涉及一系列統計衍繹之程序。剖析通常用於對人的預測，基於統計上相似之他人特質，使用各種來源之資料以推論個人。

The GDPR says that profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse *or* make predictions about individuals. The use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person.
GDPR表示，剖析係為評價個人面向而自動化運用個人資料，尤其是分析或預測個人。使用「評價」一詞表示剖析涉及對某人進行某種形式之評估或判斷。

A simple classification of individuals based on known characteristics such as their age, sex, and height does not necessarily lead to profiling. This will depend on the purpose of the classification. For instance, a business may wish to classify its customers according to their age or gender for statistical purposes and to acquire an aggregated overview of its clients without making any predictions or drawing any conclusion about an individual. In this case, the purpose is not assessing individual characteristics and is therefore not profiling.
基於已知特徵（例如年齡、性別和身高）而對當事人進行簡單分類並不一定會導向剖析。

此應取決於分類之目的。例如，企業可能希望依據年齡或性別對其客戶進行分類以用於統計目的，並獲得對客戶的整體概觀，而無需做出任何預測或得出與個人相關之任何結論。在此情況下，其目的並非評估當事人特徵，因此不屬於剖析。

The GDPR is inspired by but is not identical to the definition of profiling in the Council of Europe Recommendation CM/Rec (2010)13[2] (the Recommendation), as the Recommendation *excludes* processing that does not include inference. Nevertheless the Recommendation usefully explains that profiling may involve three distinct stages:
GDPR雖受歐盟理事會第CM / Rec（2010）13號建議書[2]（下稱建議書）啟發，但因建議書排除不涉推論之運用，因此二者對剖析的定義有所不同。然而，該建議書有效地解釋了剖析可能涉及之三種不同階段：

- data collection;
  資料蒐集；
- automated analysis to identify correlations;
  自動化分析以識別關聯性；
- applying the correlation to an individual to identify characteristics of present or future behaviour.
  將關聯性應用於個人以識別目前或未來行為之特徵。

Controllers carrying out profiling will need to ensure they meet the GDPR requirements in respect of all of the above stages.
控管者在執行剖析時將需確保符合GDPR對上述所有階段規定之要求。

Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example, their:
從廣義上來說，剖析意味著蒐集有關個人（或一群個人）之資訊並評價其特徵或行為模式，以便將其歸納入某個類型或群體，尤其是分析和/或預測，例如，他們的：

- ability to perform a task;

[2] Council of Europe. The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum. Council of Europe 23 November 2010. https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf . Accessed 24 April 2017
歐盟理事會。保護個人在剖析之背景下自動化運用個人資料。第 CM / Rec（2010）13 號建議和解釋備忘錄。歐盟理事會 2010 年 11 月 23 日。https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf . 瀏覽日期：2017年4月24日。

執行任務之能力；

- interests; or
  興趣；或
- likely behaviour.
  可能之行為。

Example
示例

A data broker collects data from different public and private sources, either on behalf of its clients or for its own purposes. The data broker compiles the data to develop profiles on the individuals and places them into segments. It sells this information to companies who wish to improve the targeting of their goods and services. The data broker carries out profiling by placing a person into a certain category according to their interests.
資料仲介代表其客戶或基於自身目的，從不同的公共和私人來源蒐集資料。資料仲介編輯資料以建立個人剖析檔案，並將其分類。仲介出售此資訊予希望改進其產品和服務之定位的公司。資料仲介透過依個人興趣分類之方式進行剖析。

Whether or not there is automated decision-making as defined in Article 22(1) will depend upon the circumstances.
是否存在第22條第1項所定義之自動化決策將取決於具體情況。

B. Automated decision-making
自動化決策

Automated decision-making has a different scope and may partially overlap with or result from profiling. Solely automated decision-making is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data, for example:
自動化決策具有不同之範圍，且可能與剖析部分重疊或因剖析而產生。純自動化決策係指在沒有人為參與之情況下，透過技術性方式做出決策之能力。自動化決策可以任何類型之資料為基礎而產生，例如：

- data provided directly by the individuals concerned (such as responses to a

questionnaire);
直接由相關個人提供之資料（如對調查問卷之回覆）；

- data observed about the individuals (such as location data collected via an application);
觀察個人所得之資料（例如透過應用程式蒐集之位置資料）；
- derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score).
衍生或推論之資料，例如由已建立之個人剖析檔案（例如，信用評分）。

Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However, profiling and automated decision-making are not necessarily separate activities. Something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used.
不論有無剖析皆可做出自動化決策；而在無自動化決策之情況下亦可執行剖析。然而，剖析和自動化決策不一定是分開的活動。某一個在剛開始時只是簡單的自動化決策程序，視其資料之使用方式，可能成為基於剖析而為之決策。

Example
示例

Imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision- making process that does not necessarily involve profiling.
僅依高速攝影機取得之證據而裁處之超速罰款，是一種不一定涉及剖析之自動化決策程序。

It would, however, become a decision based on profiling if the driving habits of the individual were monitored over time, and, for example, the amount of fine imposed is the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations.
然而，若長時間監控個人之駕駛習慣，則可能成為依據剖析之決策，例如，若罰鍰裁處額度涉及其他因素評估之結果，如超速是否為重複犯行或駕駛人最近是否有其他的交通違規行為。

Decisions that are not solely automated might also include profiling. For example, before granting a mortgage, a bank may consider the credit score of the borrower, with additional meaningful

intervention carried out by humans before any decision is applied to an individual.
非純自動化決策亦可能包含剖析。例如，在給予抵押貸款前，銀行可能會考量借款人之信用評分，而在對個人作出任何決定前，進行其他有意義之人為參與。

C. How the GDPR addresses the concepts
GDPR如何處理這些概念

There are potentially three ways in which profiling may be used:
可能有三種使用剖析之方式：

(i) general profiling;
一般剖析；

(ii) decision-making based on profiling; and
基於剖析所為之決策； 及

(iii) *solely* automated decision-making, including profiling, which produces legal effects or similarly significantly affects the data subject (Article 22[1]).
對當事人產生法律效果或類似重大影響之包含剖析的純自動化決策（第22條第1項）。

The difference between (ii) and (iii) is best demonstrated by the following two examples where an individual applies for a loan online:
（ii）和（iii）之間的差異可以個人申請線上貸款的兩個示例做最好的說明：

- a human decides whether to agree the loan based on a profile produced by purely automated means(ii);
  依據純自動化方式之剖析，由人為決定是否同意貸款（ii）；
- an algorithm decides whether the loan is agreed and the decision is automatically delivered to the individual, without any prior and meaningful assessment by a human (iii).
  以演算法決定是否同意貸款，且自動傳遞該決定予該個人，而無需任何事前且有意義的人為評估（iii）。

Controllers can carry out profiling and automated decision-making as long as they can meet all the principles and have a lawful basis for the processing. Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling, defined in Article 22(1).
控管者只要能符合所有原則並具有運用之合法基礎，即可進行剖析和自動化決策。在第22

條第1項定義之純自動化決策(包含剖析)情況下，需適用額外之安全維護措施和限制。

Chapter III of these guidelines explains the GDPR provisions for *all* profiling and automated individual decision-making. This includes decision-making processes that are *not* solely automated.
本指引第三章說明GDPR對*所有*剖析和自動化個人決策之規定。此包含*非單*純自動化決策程序。

Chapter IV of these guidelines explains the specific provisions that *only* apply to solely automated individual decision-making, including profiling.[3] A general prohibition on this type of processing exists to reflect the potential risks to individuals' rights and freedoms.
本指引第四章針對*僅*適用於純自動化個人決策(包含剖析)之具體規定進行說明。[3]為反映個人權利和自由之潛在風險，一般禁止此類運用。

III. General provisions on profiling and automated decision-making
關於剖析和自動化決策之一般規定

This overview of the provisions applies to all profiling and automated decision-making. Additional specific provisions set out in Chapter IV apply if the processing meets the definition in Article 22(1).
此規定之概述適用於所有剖析和自動化決策。若運用符合第22條第1項之定義，則適用第IV章中之額外具體規定。

A. Data protection principles
資料保護原則

The principles are relevant for all profiling and automated decision-making involving personal data.[4] To aid compliance, controllers should consider the following key areas:
這些原則與涉及個人資料之所有剖析和自動化決策相關。[4]為協助其合規，控管者應考量以下關鍵面向：

1. Article 5(1) (a) - Lawful, fair and transparent

[3] As defined in Article 22(1) of the GDPR.
如GDPR第22條第1項所定義。
[4] GDPR – Recital 72 "Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles."
GDPR－前言第 72點「剖析需符合本規則有關個人資料運用之規定，例如運用之法律依據或資料保護原則。」

第 5 條第 1 項第 a 款 - 合法、公正和透明化

Transparency of processing[5] is a fundamental requirement of the GDPR.
運用之透明度[5]為GDPR之基本要求。

The process of profiling is often invisible to the data subject. It works by creating derived or inferred data about individuals – 'new' personal data that has not been provided directly by the data subjects themselves. Individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes.
當事人通常無法察覺剖析之程序。其藉由建立有關個人之衍生或推論資料運作 － 此一「新的」個人資料並非由當事人本身直接提供。個人具有不同程度之理解能力，且可能發現要理解剖析和自動化決策程序中所涉及之複雜技術是具有挑戰性的。

Under Article 12.1 the controller must provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data.[6]
依據第12條第1項，控管者必須提供當事人有關其個人資料運用之簡潔、透明、易懂且便於取得之資訊[6]。

For data collected directly from the data subject this should be provided at the time of collection (Article 13); for indirectly obtained data the information should be provided within the timescales set out in Article 14(3).
對於直接從當事人蒐集之資料，該資訊應在蒐集時提供（第13條）；對於間接取得之資料，應在第14條第3項規定之時間範圍內提供資訊。

---

[5] The WP29 Guidelines on transparency cover transparency generally in more detail Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679 WP260, 28 November 2017 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Accessed 18 December 2017.
WP29關於透明化之指引更廣泛地涵蓋透明化之更多細節，第29條個資保護工作小組。關於第2016/679號規則中的透明化之指引（WP260），2017年11月28日。http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850，瀏覽日期：2017年12月18日。

[6] Office of the Australian Information Commissioner. Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016 says: "Privacy notices have to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. *The very technology that leads to greater collection of personal information also presents the opportunity for more dynamic, multi - layered and user centric privacy notices."* https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles . Accessed 24 April 2017
澳洲資訊委員辦公室。諮詢草案：大數據指南和澳洲隱私原則，第05/2016號指出：「隱私聲明必須清楚、簡單地傳達處理資訊之實際情形，資訊亦須具全面性及足夠之特定性，而使其有意義。正是該項*可更廣泛蒐集個人資訊之技術，亦顯示有機會可提供更加動態、多層次和以用戶為中心之隱私聲明。*」https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy- principles，造訪於2017年4月24日。

Example

示例

Some insurers offer insurance rates and services based on an individual's driving behaviour. Elements taken into account in these cases could include the distance travelled, the time spent driving and the journey undertaken as well as predictions based on other data collected by the sensors in a (smart) car. The data collected is used for profiling to identify bad driving behaviour (such as fast acceleration, sudden braking, and speeding). This information can be cross-referenced with other sources (for example the weather, traffic, type of road) to better understand the driver's behaviour.

某些保險公司依據當事人之駕駛行為提供保險費率和服務。於這些情況下考量之因素可能包含行駛距離、駕駛時間和行程、以及以（智慧）汽車中感應器蒐集之其他資料所為之預測。蒐集之資料用於剖析以識別不良駕駛行為（例如快速加速、緊急煞車和超速）。該資訊可與其他來源（例如天氣、交通、道路類型）做交叉比對，以更加了解駕駛之行為。

The controller must ensure that they have a lawful basis for this type of processing. The controller must also provide the data subject with information about the collected data, and, if appropriate, the existence of automated decision-making referred to in Article 22(1) and (4), the logic involved, and the significance and envisaged consequences of such processing.

控管者必須確保其具有此類運用之合法基礎。控管者亦須提供當事人關於所蒐集資料之資訊，並在適當情況下，提供第22條第1項和第4項所述之自動化決策、所涉邏輯以及該運用之重要性及預見之後果。

The specific requirements surrounding information and access to personal data are discussed in Chapters III (section D) and IV (section E).

有關資訊和近用個人資料之具體要求將在第III章（第D節）和第IV章（第E節）中討論。

Processing also has to be fair, as well as transparent.

運用亦須公正且透明。

Profiling may be unfair and create discrimination, for example by denying people access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products. The following example, which would not meet the requirements of Article 5(1)(a), illustrates how unfair profiling can lead to some consumers being offered less attractive

deals than others.

剖析可能係不公正的，並造成歧視，例如，拒絕人們獲得就業機會、信貸或保險，或將其作為過度風險或昂貴之金融產品的目標。以下之示例在不符合第5條第1項第a款要求之情況下，說明了不公正之剖析如何導致某些消費者被給予較不具吸引力之交易條件。

Example

示例

A data broker sells consumer profiles to financial companies without consumer permission or knowledge of the underlying data. The profiles define consumers into categories (carrying titles such as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Tough Start: Young Single Parents,") or "score" them, focusing on consumers' financial vulnerability. The financial companies offer these consumers payday loans and other "non-traditional" financial services (high-cost loans and other financially risky products).[7]

資料仲介在未經消費者許可或消費者對相關資料不知情之情況下，將消費者檔案出售予金融公司。這些檔案依消費者之財務脆弱性，將其劃分為不同之類型（名稱包含例如「鄉村和生活貧困者」、「少數民族二線城市掙扎者」、「艱難的開始：年輕單身父母」）或將其「評分」。金融公司為這些消費者提供發薪日貸款和其他「非傳統性」金融服務（高成本貸款和其他有金融風險之產品）。[7]

2. Article 5(1) (b) Further processing and purpose limitation

第 5 條第 1 項第 b 款進一步運用和目的限制

Profiling can involve the use of personal data that was originally collected for something else.

剖析可能涉及使用最初為其他目的蒐集之個人資料。

[7] This example is taken from: United States Senate, Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, December 18, 2013. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf . See page ii of the Executive Summary and 12 of the main body of the document in particular. Accessed 21 July 2017

此示例來源：美國參議院，商業、科學和運輸委員會。資料中介產業評論：因行銷目的蒐集、使用和銷售消費者資料，洛克菲勒主席之評核報告，2013 年 12 月 18 日。ttps://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577 / AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry. pdf。 請參閱摘要第 ii 頁，特別是文件本文第 12 頁，瀏覽日期：2017 年 7 月 21 日。

Example

示例

Some mobile applications provide location services allowing the user to find nearby restaurants offering discounts. However, the data collected is also used to build a profile on the data subject for marketing purposes - to identify their food preferences, or lifestyle in general. The data subject expects their data will be used to find restaurants, but not to receive adverts for pizza delivery just because the app has identified that they arrive home late. This further use of the location data may not be compatible with the purposes for which it was collected in the first place, and may thus require the consent of the individual concerned.[8]

某些行動電話應用程式提供定位服務，允許用戶可搜尋附近提供折扣的餐廳。然而，為行銷目的，所蒐集之資料亦用於建立當事人剖析檔案 - 以識別其食物偏好或一般的生活方式。當事人預期到其資料將被用於查找餐廳，但未預期到該應用程式僅因識別其回家時間較晚，就接收到外送披薩的廣告。此種定位資料之進一步使用可能與最初蒐集該資料之目的不相容，因而需要該個人之同意。[8]

Whether this additional processing is compatible with the original purposes for which the data were collected will depend upon a range of factors[9], including what information the controller initially provided to the data subject. These factors are reflected in the GDPR[10]and summarised below:

此額外運用是否與蒐集資料之原始目的相容將取決於一系列因素[9]，包含控管者最初提供予當事人之資訊。這些因素反映於GDPR中[10]，並總結如下：

- the relationship between the purposes for which the data have been collected and the purposes of further processing;

  蒐集資料之目的與進一步運用目的間之關係；

- the context in which the data were collected and the reasonable expectations of the data subjects as to their further use;

[8] Note that the provisions of the future ePrivacy Regulation may also apply.
應注意未來電子隱私規則之規定亦可能適用。

[9] Highlighted in the Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation,2 April 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . Accessed 24 April 2017
第 29 條個資保護工作小組第 03/2013 號關於目的限制之意見強調，2013 年 4 月 2 日.http：//ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommended / files / 2013 / wp203_en.pdf，瀏覽日期： 2017 年 4 月 24 日。

[10] GDPR Article 6(4).
GDPR第6條第4款。

蒐集資料之背景以及當事人對該資料進一步使用之合理期待；

- the nature of the data;
  資料之性質；
- the impact of the further processing on the data subjects; and
  進一步運用對當事人之影響；及
- the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.
  控管者實施之安全維護措施，以確保公正運用並防止對當事人產生任何不當之影響。

3. Article 5(1) (c) Data minimisation

第 5 條第 1 項第 c 款資料最小化

The business opportunities created by profiling, cheaper storage costs and the ability to process large amounts of information can encourage organisations to collect more personal data than they actually need, in case it proves useful in the future. Controllers must make sure they are complying with the data minimisation principle, as well as the requirements of the purpose limitation and storage limitation principles.

剖析所帶來的商機、更低廉的儲存成本和運用大量資訊之能力皆鼓勵組織蒐集比實際所需更多之個人資料，以為將來可能之使用。控管者必須確保其符合資料最小化原則，以及目的限制和儲存限制原則之要求。

Controllers should be able to clearly explain and justify the need to collect and hold personal data, or consider using aggregated, anonymised or (when this provides sufficient protection) pseudonymised data for profiling.

控管者必須能夠清楚地說明和證明蒐集及持有個人資料之必要性，或考量使用聚集的、匿名化、或（當提供足夠保護時）假名化資料進行剖析。

4. Article 5(1) (d) Accuracy

第 5 條第 1 項第 d 款正確性

Controllers should consider accuracy at all stages of the profiling process, specifically when:

控管者應在剖析程序的所有階段考量正確性，尤其是在：

- collecting data;
  蒐集資料；
- analysing data;

分析資料；

- building a profile for an individual; or
  建立個人剖析檔案；或
- applying a profile to make a decision affecting the individual.
  使用剖析檔案做出影響個人之決策。

If the data used in an automated decision-making or profiling process is inaccurate, any resultant decision or profile will be flawed. Decisions may be made on the basis of outdated data or the incorrect interpretation of external data. Inaccuracies may lead to inappropriate predictions or statements about, for example, someone's health, credit or insurance risk.
若自動化決策或剖析程序中使用之資料不正確，任何由此產生之決策或剖析檔案都將存在缺陷。決策可能依據過時之資料或對外部資料之錯誤解釋而產生。不正確性可能導致例如對某人健康、信用或保險風險之不當預測或陳述。

Even if raw data is recorded accurately, the dataset may not be fully representative or the analytics may contain hidden bias.
即使原始資料正確紀錄，其資料集可能不具備完全之代表性，或其分析可能包含隱藏性之偏見。

Controllers need to introduce robust measures to verify and ensure on an ongoing basis that data re- used or obtained indirectly is accurate and up to date. This reinforces the importance of providing clear information about the personal data being processed, so that the data subject can correct any inaccuracies and improve the quality of the data.

控管者需採行強力之措施持續驗證並確保再使用或間接取得之資料係正確和最新的。此加強了提供所運用個人資料的清楚資訊之重要性，如此可使當事人更正任何不正確資料並提高資料品質。

5. Article 5(1) (e) Storage limitation
第 5 條第 1 項第 e 款儲存限制

Machine-learning algorithms are designed to process large volumes of information and build correlations that allow organisations to build up very comprehensive, intimate profiles of individuals. Whilst there can be advantages to retaining data in the case of profiling, since there will be more data for the algorithm to learn from, controllers must comply with the data minimisation principle when they collect personal data and ensure that they retain those personal data for no longer than is necessary for and proportionate to the purposes for which the personal data are processed.
機器學習演算法之設計係在運用大量資訊並建立關聯性，使組織建立非常全面性、私密性

之個人剖析檔案。雖然在剖析時保留資料可能會有好處，因會有更多之資料供演算法學習，然而控管者在蒐集個人資料時必須遵守資料最小化原則，並確保其保留這些個人資料不超過個人資料運用目的所必須，且符合比例性。

The controller's retention policy should take into account the individuals' rights and freedoms in line with the requirements of Article 5(1)(e).
控管者之資料保留政策應依據第5條第1項第e款之要求考量個人之權利和自由。

The controller should also make sure that the data remains updated throughout the retention period to reduce the risk of inaccuracies.[11]
控管者亦應確保資料在保留期限內維持更新，以降低不正確之風險。[11]

B. Lawful bases for processing
運用之合法依據

Automated decision-making defined in Article 22(1) is only permitted if one of the exceptions described in Chapter IV (sections C and D) applies. The following lawful bases for processing are relevant for all other automated individual decision-making and profiling.
只有在適用第IV章（第C和D節）所描述之例外情形下，始允許執行第22條第1項規定之自動化決策。以下運用之法律依據與所有其他自動化個人決策及剖析相關。

1. Article 6(1) (a) consent
第 6 條第 1 項第 a 款同意

Consent as a basis for processing generally is addressed in the WP29 Guidelines on consent.[12] Explicit consent is one of the exceptions from the prohibition on automated decision-making and profiling defined in Article 22(1).
以同意作為運用之法律基礎一般已列入WP29關於同意之指引。[12]明確同意為第22條第1項

[11] Norwegian Data Protection Authority. The Great Data Race – How commercial utilisation of personal data challenges privacy, Report, November 2015. Datatilsynet https://www.datatilsynet.no/English/Publications/The- Great-Data-Race/ Accessed 24 April 2017[12] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679 WP259, 28 November 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accessed 18 December 2017
挪威資料保護機關。大數據競賽 - 個人資料商業利用對隱私權之挑戰，報告，2015 年 11 月。Datatilsynet https://www.datatilsynet.no/English/Publications/The- Great-Data-Race / 瀏覽日期：2017 年 4 月 24 日。第 29 條個資保護工作小組，關於第 2016/179 號規則中的同意之指引（WP259），2017 年 11 月 28 日，http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849。 造訪於 2017 年 12 月 18 日。

[12] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679 WP259, 28 November 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accessed 18 December 2017
第29條個資保護工作小組。第2016/679號規則關於同意之指引，WP259，2017年11月28日，http：

禁止自動化決策和剖析的例外情況之一。

Profiling can be opaque. Often it relies upon data that is derived or inferred from other data, rather than data directly provided by the data subject.
剖析可能是不透明的。剖析經常依賴從其他資料衍伸或推論而來之資料，而非由當事人直接提供之資料。

Controllers seeking to rely upon consent as a basis for profiling will need to show that data subjects understand exactly what they are consenting to, and remember that consent is not always an appropriate basis for the processing.[13] In all cases, data subjects should have enough relevant information about the envisaged use and consequences of the processing to ensure that any consent they provide represents an informed choice.
控管者若尋求以同意作為剖析依據，需證明當事人完全理解其同意之內容，且切記同意非必為運用之適當依據。[13]在所有情況下，當事人就預期使用及運用的結果應有足夠之相關資訊，以確保其提供之任何同意係屬告知後的選擇。

2. Article 6(1) (b) – necessary for the performance of a contract
第 6 條第 1 項第 b 款 – 為履行契約所必須

Controllers may wish to use profiling and automated decision-making processes because they:
控管者可能希望使用剖析和自動化決策程序，因其：

- potentially allow for greater consistency or fairness in the decision making process (e.g. by reducing the potential for human error, discrimination and abuse of power);
  可能使決策程序更具一致性或公正性（例如，透過減少潛在之人為錯誤、歧視和濫用權力）；
- reduce the risk of customers failing to meet payments for goods or services (for example by using credit referencing); or
  降低客戶未能支付商品或服務之風險（例如透過信用參考）；或
- enable them to deliver decisions within a shorter time frame and improve efficiency.
  使控管者能在更短的時間內做出決策並提高效率。

Regardless of the above, these considerations alone are not sufficient to show that this type of processing is *necessary* under Article 6(1)(b) for the performance of a contract. As described in the WP29 Opinion on legitimate interest[14], necessity should be interpreted narrowly.

//ec.europa.eu/newsroom/just/document.cfm？doc_id＝48499，瀏覽日期：2017年12月18日。
[13] Ibid.
同上。

無論如何，單單這些考量並不足以證明此種運用係為履行依據第6條第1項第b款之契約*所必須*。正如WP29關於正當利益之意見所述[14]，必要性必須被限縮解釋。

The following is an example of profiling that would *not* meet the Article 6(1)(b) basis for processing.

*以下為未*符合第6條第1項第b款運用依據規定剖析之示例。

Example

示例

A user buys some items from an on-line retailer. In order to fulfil the contract, the retailer must process the user's credit card information for payment purposes and the user's address to deliver the goods. Completion of the contract is not dependent upon building a profile of the user's tastes and lifestyle choices based on his or her visits to the website. Even if profiling is specifically mentioned in the small print of the contract, this fact alone does not make it 'necessary' for the performance of the contract.

用户從網路零售商購買某些商品。為了履行契約，零售商必須運用用户之信用卡資訊支付和用户地址以交付貨物。契約之完成並不仰賴依據用户造訪網站之行為而建立用户喜好和生活方式選擇之剖析檔案。即使在契約中以小字體特別提及剖析，僅此一事實並會使剖析成為履行契約所「必須」。

3. Article 6(1) (c) – necessary for compliance with a legal obligation

第 6 條第 1 項第 c 款 – 為履行法律義務所必須

There may be instances where there will be a legal obligation[15] to carry out profiling – for example in connection with fraud prevention or money laundering. The WP29 Opinion on legitimate interests[16] provides useful information about this basis for processing, including the safeguards to be applied.

在某些情況下，可能會依法律義務[15]而執行剖析 - 例如與預防詐欺或洗錢相關聯時。WP29關於正當利益[16]之意見提供了與此一運用基礎相關之有用資訊，包含應適用之安全維護措

[14] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. European Commission, 9 April 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp 217_en.pdf . Accessed 24 April 2017

第06/2014號意見依據第95/46/EC號指令第7條關於資料控管者正當利益之見解。歐盟執委會，2014年4月9日.http：//ec.europa.eu/justice/data-protection/article- 29 / documentation / opinion-recommendation / files / 2014 / wp 217_en.pdf。瀏覽日期： 2017年4月24日。

[15] GDPR Recitals 41 and 45.

GDPR前言第41和45點。

[16] Page 19 Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate

施。

4. Article 6(1) (d) – necessary to protect vital interests

第 6 條第 1 項第 d 款 － 為保護重大利益所必須

This covers situations where the processing is necessary to protect an interest which is essential for the life of the data subject or that of another natural person.

此包含當運用為保護當事人或另一自然人生命重要利益所必須之情況。

Certain types of processing may serve important public interest grounds as well as the vital interests of the data subject. Examples of this may include profiling necessary to develop models that predict the spread of life-threatening diseases or in situations of humanitarian emergencies. In these cases, however, and in principle, the controller can only rely on vital interest grounds if no other legal basis for the processing is available.[17] If the processing involves special category personal data the controller would also need to ensure that they meet the requirements of Article 9(2) (c).

某些類型之運用可能係為重要公共利益以及當事人之重大利益。這些情況之示例可能包含當剖析對開發預測威脅生命疾病之模型或人道主義緊急情況為必須時。然而，在這些情況下，原則上，控管者只有在沒有其他適合之運用法律依據時，始得以重要利益為理由。[17]若運用涉及特種個人資料，控管者亦需確保其符合第9條第2項第c款之要求。

5. Article 6(1) (e) – necessary for the performance of a task carried out in the public interest or exercise of official authority

第 6 條第 1 項第 e 款 － 因履行公共利益或行使公權力而執行任務所必須

Article 6(1) (e) might be an appropriate basis for public sector profiling in certain circumstances. The task or function must have a clear basis in law.

在某些情況下，第6條第1項第e款可作為公部門執行剖析之適當基礎。然其任務或職能必須在法律上有明確之基礎。

6. Article 6(1) (f) – necessary for the legitimate interests[18] pursued by the controller or by a third party

第 6 條第 1 項第 f 款 － 為控管者或第三方追求正當利益[18]所必須

---

interests of the data controller under Article 7 of Directive 95/46/EC. European Commission, 9 April 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Accessed 24 April 2017

第29條個資保護工作小組第19頁。第95/46 / EC號指令第7條關於資料控管者正當利益概念第06/2014號意見。歐盟執委會，2014年4月9日 http：//ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation / files / 2014 / wp 217_en.pdf。瀏覽日期： 2017年4月24日。

[17] GDPR Recital 46

GDPR前言第46點。

[18] Legitimate interests listed in GDPR Recital 47 include processing for direct marketing purposes and

Profiling is allowed if it is necessary for the purposes of the legitimate interests[19] pursued by the controller or by a third party. However, Article 6(1) (f) does not automatically apply just because the controller or third party has a legitimate interest. The controller must carry out a balancing exercise to assess whether their interests are overridden by the data subject's interests or fundamental rights and freedoms.

若為控管者或第三方追求正當利益[19]之目的所必須，可執行剖析。然而，第6條第1項第f款並不僅因控管者或第三方擁有正當利益而自動適用。控管者必須進行平衡判斷，以評估其利益是否為當事人利益或基本權利和自由所超越。

The following are particularly relevant:

下述幾點尤為相關：

- the level of detail of the profile (a data subject profiled within a broadly described cohort such as 'people with an interest in English literature', or segmented and targeted on a granular level);
  剖析檔案之詳盡程度（當事人被剖析歸類在某個廣泛描述族群，例如「對英語文學感興趣的人」，或在細度層級進行劃分和目標鎖定）；
- the comprehensiveness of the profile (whether the profile only describes a small aspect of the data subject, or paints a more comprehensive picture);
  剖析檔案之全面性（剖析檔案是否僅描述與當事人相關之一小部分，或是更加全面性的描繪）；
- the impact of the profiling (the effects on the data subject); and
  剖析之影響（對當事人之影響）；及
- the safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process.
  旨在確保剖析程序之公正、無歧視和正確之安全維護措施。

Although the WP29 opinion on legitimate interests[20] is based on Article 7 of the data protection Directive 95/46/EC (the Directive), it contains examples that are still useful and relevant for controllers carrying out profiling. It also suggests it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across

---

processing strictly necessary for the purposes of preventing fraud.
GDPR前言第47點所列舉之正當利益包含為行銷目的之運用和為防止欺詐之目的而確實必要之運用。

[19] The controller's "legitimate interest" cannot render profiling lawful if the processing falls within the Article 22(1) definition.
若運用屬於第22條第1項之範圍，則控管者之「正當利益」不得作為剖析之合法依據。

multiple websites, locations, devices, services or data-brokering.
儘管WP29關於正當利益[20]之意見係基於第95/46/EC號資料保護指令（指令）第7條，然其涵蓋之示例對於執行剖析之控管者仍有效且相關。該意見亦表明，當控管者為行銷或廣告目的而執行侵入性剖析和追蹤活動時，很難使用正當利益作為合法依據，例如涉及跨越多個網站、位置、設備、服務或資料仲介而追蹤當事人之控管者。

The controller should also consider the future use or combination of profiles when assessing the validity of processing under Article 6(1) (f).
在評估第6條第1項第f款運用之有效性時，控管者亦應考量對剖析檔案未來之使用或組合。

C. Article 9 – Special categories of data
第9條 － 特種資料

Controllers can only process special category personal data if they can meet one of the conditions set out in Article 9(2), as well as a condition from Article 6. This includes special category data derived or inferred from profiling activity.
控管者須符合第9條第2項規定要件之一以及第6條之規定，始可運用特種個資。此包含從剖析活動中衍伸或推論之特種資料。

Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods.
剖析可透過資料推論以建立特種資料，這些推論資料本身並非特種資料，然當與其他資料結合時即成為特種資料。例如，可從個人食品購物記錄結合食品質量和能量含量之資料以推論其健康情況。

Correlations may be discovered that indicate something about individuals' health, political convictions, religious beliefs or sexual orientation, as demonstrated by the following example:
關聯性之發現可指出當事人的健康狀況、政治理念、宗教信仰或性取向，如下例所示：

[20] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. European Commission, 9 April 2014, Page 47, examples on pages 59 and 60 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Accessed 24 April 2017
第 29 條個資保護工作小組。第 95/46 / EC 號指令第 7 條關於資料控管者正當利益概念第 06/2014 號意見。歐盟執委會，2014 年 4 月 9 日，第 47 頁，第 59 和 60 頁中之示例 http://ec.europa.eu/justice/data-protection/article-29 / documentation / opinion-recommendation / files / 2014 / wp 217_en.pdf。瀏覽日期： 2017 年 4 月 24 日。

Example
示例

One study[21] combined Facebook 'likes' with limited survey information and found that researchers accurately predicted a male user's sexual orientation 88% of the time; a user's ethnic origin 95% of the time; and whether a user was Christian or Muslim 82% of the time.
一項研究[21]將Facebook的「讚」與有限的調查資訊相結合，發現研究人員準確地預測了88%男性用戶性取向；95%用戶種族來源；82%用戶是基督徒或穆斯林教徒。

If sensitive preferences and characteristics are inferred from profiling, the controller should make sure that:
若從剖析中推論出敏感之個人偏好和特徵，控管者應確保：

- the processing is not incompatible with the original purpose;
  運用與原始目的不會不相容；
- they have identified a lawful basis for the processing of the special category data; and
  確認了運用特種資料之合法依據；及
- they inform the data subject about the processing.
  已就相關運用告知當事人。

Automated decision-making as defined in Article 22(1) that is based on special categories of data is covered in Chapter IV (section D).
第IV章（第D節）涵蓋了第22條第1項所定義之基於特種資料所為之自動化決策。

D. Rights of the data subject[22]
當事人之權利[22]

The GDPR introduces stronger rights for data subjects and creates new obligations for

[21] Michael Kosinski, David Stilwell and Thore Graepel. Private traits and attributes are predictable from digital records of human behaviour. Proceedings of the National Academy of Sciences of the United States of America, http://www.pnas.org/content/110/15/5802.full.pdf . Accessed 29 March 2017.
Michael Kosinski，David Stilwell和Thore Graepel。私人特徵和屬性可從人類行為之數位記錄預測。美國國家科學院會議記錄，http：//www.pnas.org/content/110/15/5802.full.pdf。瀏覽日期： 2017年3月29日。

[22] This Section is relevant for both profiling and automated decision-making. For automated decision making under Article 22, please note that there are also additional requirements as described in Chapter IV.
本章節與剖析和自動化決策相關。對於第22條規定下之自動化決策，請注意第IV章中就此尚有其他要求。

controllers.
GDPR加強了當事人之權利，並對控管者加諸新的義務。

In the context of profiling these rights are actionable against the controller creating the profile and the controller making an automated decision about a data subject (with or without human intervention), if these entities are not the same.
在剖析之背景下，當事人對於建立剖析檔案之控管者和做出關於當事人之自動化決策（無論是否有人為參與）的控管者（若兩者非同一控管者），均得行使權利。

Example
示例

A data broker undertakes profiling of personal data. In line with their Article 13 and 14 obligations the data broker should inform the individual about the processing, including whether they intend to share the profile with any other organisations. The data broker should also present separately details of the right to object under Article 21(1).
資料仲介從事對個人資料之剖析。依據第13條和第14條之義務，資料仲介應就相關運用告知當事人，包括其是否打算與任何其他組織共享該剖析檔案。資料仲介亦應單獨詳列出第21條第1項所規定之拒絕權。

The data broker shares the profile with another company. This company uses the profile to send the individual direct marketing.
資料仲介與另一家公司共享剖析檔案。而該公司使用此檔案對當事人行銷。

The company should inform the individual (Article 14(1) (c)) about the purposes for using this profile, and from what source they obtained the information (14(2) (f)). The company must also advise the data subject about their right to object to processing, including profiling, for direct marketing purposes (Article 21(2)).
該公司應告知當事人（第14條第1項第c款）關於使用剖析檔案之目的，以及從何處獲得此資訊（第14條第2項第f款）。該公司亦須向當事人告知有關拒絕運用(包括為行銷目的之剖析) 之權利（第21條第2項）。

The data broker and the company should allow the data subject the right to access the information used (Article 15) to correct any erroneous information (Article 16), and in certain circumstances erase the profile or personal data used to create it (Article 17). The data subject should also be given information about their profile, for example in which 'segments' or 'categories' they are placed. [23]

資料仲介和公司應允許當事人有權近用其被使用之資訊（第15條）、更正任何錯誤資訊（第16條），並在某些情況下刪除剖析檔案或用以建立該檔案之個人資料（第17條）。另亦應提供當事人其剖析檔案之相關資訊，例如被分置於何種「分類」或「類型」之資訊。[23]

If the company uses the profile as part of a solely automated decision-making process with legal or similarly significant effects on the data subject, the company is the controller subject to the Article 22 provisions. (This does not exclude the data broker from Article 22 if the processing meets the relevant threshold.)

若公司使用該剖析檔案作為純自動化決策程序之一部分，而對當事人產生法律或類似重大之影響時，該公司則屬於受第22條規定拘束之控管者。（若運用符合相關門檻時，亦不排除第22條對資料仲介之適用。）

1. Articles 13 and 14 – Right to be informed
第 13 條和第 14 條 - 被告知權

Given the core principle of transparency underpinning the GDPR, controllers must ensure they explain clearly and simply to individuals how the profiling or automated decision-making process works.

鑑於「透明」為GDPR之核心原則，控管者必須確保向當事人清晰且簡單地說明剖析或自動化決策程序之運作。

In particular, where the processing involves profiling-based decision making (irrespective of whether it is caught by Article 22 provisions), then the fact that the processing is for the purposes of both (a) profiling and (b) making a decision based on the profile generated, must be made clear to the data subject.[24]

尤其是，若運用涉及基於剖析而為之決策（無論是否適用第22條之規定），則必須向當事人清楚表明運用之目的是為了（a）剖析及（b）以該剖析檔案而作出決策。[24]

---

[23] The Norwegian Data Protection Authority. The Great Data Race -How commercial utilisation of personal data challenges privacy. Report, November 2015. https://www.datatilsynet.no/English/Publications/The-Great-Data- Race/ Accessed 24 April 2017
挪威資料保護機關。大數據競賽 - 個人資料之商業利用對隱私權之挑戰。報告，2015年11月。https://www.datatilsynet.no/English/Publications/The- Great-Data-Race / 瀏覽日期：2017年4月24日。

[24] GDPR – Article 13(1)(c) and Article 14(1)(c). Article 13(2)(f) and 14(2)(g) require the controller to inform the data subject about the existence of automated decision-making, including profiling, described in Article 22(1) and (4). This is explained further in Chapter IV.
GDPR－ 第13條第1項第c款和第14條第1項第c款。第13條第2項第f款和第14條第2項第g款要求控管者告知當事人有關第22條第1項和第4項所述自動化決策之存在(包含剖析)。將在第IV章對此作進一步說明。

Recital 60 states that giving information about profiling is part of the controller's transparency obligations under Article 5(1) (a). The data subject has a right *to be informed* by the controller about and, in certain circumstances, a right *to object to* 'profiling', *regardless* of whether solely automated individual decision-making based on profiling takes place.

前言第60點指出，提供有關剖析之資訊係控管者依據第5條第1項第a款規定下透明義務之一部分。*無論*是否發生以剖析為基礎之純自動化個人決策，當事人有權*獲得*控管者之*告知*，並在某些情況下，有權*拒絕*「剖析」。

Further guidance on transparency in general is available in the WP29 Guidelines on transparency under the GDPR[25].

WP29關於GDPR之透明化之指引為透明化提供了進一步指導[25]。

2. Article 15 – Right of access

第 15 條 – 近用權

Article 15 gives the data subject the right to obtain details of any personal data used for profiling, including the categories of data used to construct a profile.

第15條規定當事人有權獲得任何用於剖析之個人資料的詳細資訊，包含用於建構剖析檔案之資料類型。

In addition to general information about the processing, pursuant to Article 15(3), the controller has a duty to make available the data used as input to create the profile as well as access to information on the profile and details of which segments the data subject has been placed into.

除了關於運用之一般資訊外，依據第15條第3項，控管者有責任提供用作建立剖析檔案之輸入資料，以及提供對該剖析檔案資訊之近用和當事人被歸入分類之細節。

This differs from the right to data portability under Article 20 where the controller only needs to communicate the data provided by the data subject or observed by the controller and not the profile itself.[26]

此與第20條規定之資料可攜權不同，在第20條中，控管者僅需傳遞由當事人提供或由控管者觀察所得之資料，而不包含剖析檔案本身。[26]

---

[25] Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679 WP260, 28 November 2017 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Accessed 18 December 2017.
第29條個資保護工作小組。關於第2016/679號規則之透明化指引(WP260)，2017年11月28日 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850，瀏覽日期：2017年12月18日。

[26] Page 9, WP29 Guidelines on the Right to data portability, WP242 http://ec.europa.eu/newsroom/document.cfm?doc_id=45685. Accessed 8 January 2018
第9頁，WP29關於資料可攜權指引，WP242。http://ec.europa.eu/newsroom/document.cfm?doc_id=45685。瀏覽日期：2018年1月8日。

Recital 63 provides some protection for controllers concerned about revealing trade secrets or intellectual property, which may be particularly relevant in relation to profiling. It says that the right of access 'should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software'. However, controllers cannot rely on the protection of their trade secrets as an excuse to deny access or refuse to provide information to the data subject.

當剖析與揭露營業秘密或智慧財產權尤為相關時，前言第63點為控管者提供了一些保護。該前言規定，近用權「不應對他人之權利或自由產生不利影響，包含營業秘密或智慧財產權，尤其是保護軟體著作權」。然而，控管者不能以保護其營業秘密作為拒絕近用或拒絕向當事人提供資訊之理由。

Recital 63 also specifies that 'where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.'

前言第63點亦指出「在可能之情況下，控管者應能夠提供對安全系統之遠端存取，而該系統將使當事人能夠直接近用其個人資料。」

3. Article 16 - Right to rectification, Article 17 Right to erasure and Article 18 Right to restriction of processing

第 16 條 － 更正權、第 17 條刪除權和第 18 條限制運用權

Profiling can involve an element of prediction, which increases the risk of inaccuracy. The input data may be inaccurate or irrelevant, or taken out of context. There may be something wrong with the algorithm used to identify correlations.

剖析可能涉及預測因素，因而增加不正確之風險。輸入的資料可能不正確或不相關，或脫離脈絡。而用於識別關聯性之演算法可能存在某些問題。

The Article 16 right to rectification might apply where, for example, an individual is placed into a category that says something about their ability to perform a task, and that profile is based on incorrect information. Individuals may wish to challenge the accuracy of the data used and any grouping or category that has been applied to them.

第16條之更正權可適用於如，當事人就執行任務之能力被分類，然而該剖析檔案所依據之資訊不正確。當事人可能希望對所使用資料之正確性以及所被歸類劃分之任何組別或類型提出異議。

The rights to rectification and erasure[27] apply to both the 'input personal data' (the personal data used to create the profile) and the 'output data' (the profile itself or 'score' assigned to the person).

更正和刪除之權利[27]適用於「輸入之個人資料」（用於建立剖析檔案之個人資料）以及「輸出之資料」（剖析檔案本身或給予當事人之「評分」）。

Article 16 also provides a right for the data subject to complement the personal data with additional information.

第16條亦賦予當事人得以額外資訊補充個人資料之權利。

Example

示例

A local surgery's computer system places an individual into a group that is most likely to get heart disease. This 'profile' is not necessarily inaccurate even if he or she never suffers from heart disease. The profile merely states that he or she is *more likely* to get it. That may be factually correct as a matter of statistics.

一個地區外科電腦系統將某當事人歸類於最容易罹患心臟病之群體中。即使該當事人從未患有心臟病，此種「剖析」也不一定不正確。該檔案僅指出其更*有可能*罹患心臟病。就統計而言，此歸類可能事實上是正確的。

Nevertheless, the data subject has the right, taking into account the purpose of the processing, to provide a supplementary statement. In the above scenario, this could be based, for example, on a more advanced medical computer system (and statistical model) factoring in additional data and carrying out more detailed examinations than the one at the local surgery with more limited capabilities.

然而，當事人有權利在考量運用目的之情況下提供補充聲明。在上述情境中，其可依據如更先進之醫學電腦系統（和統計模型），納入其他資料，並進行比能力有限的地區外科更詳盡之檢查。

The right to restrict processing (Article 18) will apply to any stage of the profiling process.

限制運用之權利（第18條）將適用於剖析程序中之任何階段。

4. Article 21 – Right to object

第 21 條 － 拒絕權

The controller has to bring details of the right to object under Article 21(1) and (2) *explicitly* to the data subject's attention, and present it clearly and separately from other information (Article 21(4)).

[27] GDPR – Article 17[28] GDPR- Article 18(1)(d).
GDPR－ 第 17 條 GDPR－ 第 18 條第 1 項第 d 款。

控管者必須*清楚地*使當事人注意到第21條第1項和第2項所規定拒絕權之細節，並將其與其他資訊明確且分開呈現（第21條第4項）。

Under Article 21(1) the data subject can object to processing (including profiling), on grounds relating to his or her particular situation. Controllers are specifically required to provide for this right in all cases where processing is based on Article 6(1) (e) or (f).
依據第21條第1項，當事人可因與其相關之特定情況而拒絕運用（包含剖析）。當運用係依據第6條第1項第e款或f款之所有情況下，特別要求控管者提供此項權利。

Once the data subject exercises this right, the controller must interrupt[28] (or avoid starting) the profiling process unless it can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of the data subject. The controller may also have to erase the relevant personal data.[29]
一旦當事人行使此項權利，控管者就必須中斷[28]（或避免啟動）剖析程序，除非其可提出具說服性之正當理由超越當事人之利益、權利和自由。控管者可能亦須刪除相關個人資料。[29]

The GDPR does not provide any explanation of what would be considered compelling legitimate grounds. [30] It may be the case that, for example, the profiling is beneficial for society at large (or the wider community) and not just the business interests of the controller, such as profiling to predict the spread of contagious diseases.
GDPR並無提供任何有關具說服性正當理由之說明。[30]可能之情況為，例如，剖析有益於整個社會（或更廣泛之社群），而不僅係控管者之商業利益，例如預測傳染病蔓延之剖析。

The controller would need to:
控管者可能必須：

- consider the importance of the profiling to their particular objective;
  考量剖析對其特定目的之重要性;

[28] GDPR- Article 18(1)(d).
GDPR - 第18條第1項第d款。
[29] GDPR – Article 17(1)(c).
GDPR - 第17條第1第c款。
[30] See explanation on legitimacy, Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 9 April 2014. Page 24 - 26 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Accessed 24 April 2017
請參正當性之說明，第29條個資保護工作小組第95/46/EC號指令第7條關於資料控管者之正當利益概念第06/2014號意見。2014年4月9日。第24－26頁 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommended / files / 2014 / wp217_en.pdf。瀏覽日期： 2017年4月24日。

- consider the impact of the profiling on the data subject's interest, rights and freedoms – this should be limited to the minimum necessary to meet the objective; and
  考量剖析對當事人利益、權利和自由之影響 – 此應限於為達到目的所需之最小程度；及
- carry out a balancing exercise.
  進行平衡使用。

There must always be a balancing exercise between the competing interests of the controller and the basis for the data subject's objection (which may be for personal, social or professional reasons). Unlike in the Directive 95/46/EC, the burden of proof to show compelling legitimate grounds lies with the controller rather than the data subject.
在控管者的競爭利益和當事人的拒絕權利基礎（此可能是基於個人、社會或專業原因）間必須始終存在一種平衡判斷。不同於第95/46/EC號指令，提供具說服力正當理由之舉證責任在於控管者而非當事人。

It is clear from the wording of Article 21 that the balancing test is different from that found in Article 6(1)(f). In other words, it is not sufficient for a controller to just demonstrate that their earlier legitimate interest analysis was correct. This balancing test requires the legitimate interest to be *compellin*g, implying a higher threshold for overriding objections.
從第21條的措辭可清楚地看出，平衡測試與第6條第1項第f款之規定不同。易言之，若控管者僅提出其先前正當利益分析為正確並不足夠。此種平衡測試要求正當利益具*說服力*，此意味著若要推翻拒絕權須符合更高之門檻。

Article 21(2) grants an *unconditional* right for the data subject to object to the processing of their personal data for direct marketing purposes, including profiling to the extent that it is related to such direct marketing.[31] This means that there is no need for any balancing of interests; the controller must respect the individual's wishes without questioning the reasons for the objection. Recital 70 provides additional context to this right and says that it may be exercised at any time and free of charge.
第21條第2項賦予當事人得*無條件*拒絕為行銷目的運用其個人資料之權利，包含與此類行銷相關之剖析[31]。此意味著不需進行任何利益平衡判斷；控管者必須尊重當事人意願，而

[31] In line with Article 12(2) controllers who collect personal data from individuals with the aim of using it for direct marketing purposes should, at the moment of collection, consider offering data subjects an easy way to indicate that they do not wish their personal data to be used for direct marketing purposes, rather than requiring them to exercise their right to object at a later occasion.
依據第12條第2項，當控管者基於行銷目的而由當事人處蒐集個人資料，在蒐集資料同時，應考量提供當事人便捷之方式以表明不希望個人資料被使用於行銷之目的，而非要求當事人於其後之時點行使拒絕權。

不得質疑拒絕之理由。前言第70點為拒絕權提供了額外之背景，並表示可在任何時間無償行使該權利。

IV. Specific provisions on solely automated decision- making as defined in Article 22
第22條所定義之純自動化決策之具體規定

Article 22(1) says
第22條第1項規定

> The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces *legal effects* concerning him or her or *similarly significantly affects him or her*.
> 對當事人產生*法律效果*或*類似重大影響*之純自動化決策（包含剖析），當事人有不受拘束的權利。

The term "right" in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data.
該條款中「權利」一詞並不意味著第22條第1項僅適用於當事人主動行使之情況。第22條第1項針對純粹基於自動化運用之決策，建立了一般性的禁止原則。此種禁止之適用無關當事人是否對其個人資料之運用採取行動。

In summary, Article 22 provides that:
綜上所述，第22條規定：

(i) as a rule, there is a general prohibition on fully automated individual decision-making, including profiling that has a legal or similarly significant effect;
作為原則規範，當決策可產生法律或類似重大之影響時，通常禁止完全自動化的個人決策（包含剖析）；

(ii) there are exceptions to the rule;
該原則規範具有例外;

(iii) where one of these exceptions applies, there must be measures in place to safeguard the data subject's rights and freedoms and legitimate interests[32].
若適用其中一項例外情形，則必須採取安全維護措施確保當事人之權利和自由以

及正當利益[32]。

This interpretation reinforces the idea of the data subject having control over their personal data, which is in line with the fundamental principles of the GDPR. Interpreting Article 22 as a prohibition rather than a right to be invoked means that individuals are automatically protected from the potential effects this type of processing may have. The wording of the Article suggests that this is the intention and is supported by Recital 71 which says:

此種解釋強化了當事人得控制其個人資料之概念，此亦符合GDPR之基本原則。將第22條解釋為禁止而非被行使之權利，意味著當事人就此類運用可能產生之潛在影響會自動受到保護。該條文之措辭表明此一意圖，而前言第71點亦加以支持，並指出：

> However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law……, or necessary for the entering or performance of a contract……., or when the data subject has given his or her explicit consent
> 然而，在歐盟或成員國法律明確授權之情況下.....或為簽訂或履行契約所必須.....或當事人給予明確同意時，應允許基於此種運用所為之決策（包含剖析）。

This implies that processing under Article 22(1) is not allowed generally.[33]

此意味著原則不允許依據第22條第1項所為之運用。[33]

However the Article 22(1) prohibition *only* applies in specific circumstances when a decision based solely on automated processing, including profiling, has a legal effect on or similarly significantly affects someone, as explained further in the guidelines. Even in these cases there are defined exceptions which allow such processing to take place.

然而，如本指引進一步之解釋，第22條第1項之禁止*僅*適用於特定情況，即當基於純自動運用之決策（包含剖析）對當事人產生法律效果或類似重大影響時。即使在這些情況下，亦存在允許進行此類運用之明確例外情形。

The required safeguarding measures, discussed in more detail below, include the right to be informed (addressed in Articles 13 and 14 – specifically meaningful information about the logic involved, as well as the significance and envisaged consequences for the data subject), and

---

[32] Recital 71 says that such processing should be "subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."
前言第71點表示，此類運用應「基於適當安全維護措施，其中應包含當事人之具體資訊以及取得人為參與、表達觀點、取得評估後所作決策之理由、和質疑該決策之權利。」

[33] Further comments on the interpretation of Article 22 as a prohibition can be found in Annex 2.
關於第22條作為禁止規則解釋之進一步評論請參閱附錄2。

safeguards, such as the right to obtain human intervention and the right to challenge the decision (addressed in Article 22(3)).

下文將詳細討論所需之安全維護措施，包含被告知之權利（規定於第13條和第14條 － 尤其是關於所涉邏輯之有意義資訊，以及對當事人之重要性及預設之後果）及安全維護措施，例如取得人為參與之權利和對決策提出異議之權利（規定於第22條第3項）。

Any processing likely to result in a high risk to data subjects requires the controller to carry out a Data Protection Impact Assessment (DPIA).[34] As well as addressing any other risks connected with the processing, a DPIA can be particularly useful for controllers who are unsure whether their proposed activities will fall within the Article 22(1) definition, and, if allowed by an identified exception, what safeguarding measures must be applied.

任何可能造成當事人高風險之運用皆要求控管者辦理個資保護影響評估（DPIA）。[34]除可因應與運用相關之任何其他風險外，對不確定所擬活動是否屬於第22條第1項之定義範圍，或當該活動屬於明確例外情形時應採取何種安全維護措施，DPIA尤其可提供控管者協助。

A ‘Decision based solely on automated processing’ 「基於純自動化運用之決策」

Article 22(1) refers to decisions ‘based solely’ on automated processing. This means that there is no human involvement in the decision process.

第22條第1項係指「純基於」自動化運用之決策。此意味著決策程序中並無人為參與。

Example

示例

An automated process produces what is in effect a recommendation concerning a data subject. If a human being reviews and takes account of other factors in making the final decision, that decision would not be ‘based solely’ on automated processing.

自動化程序可產生實際上與當事人相關之建議。若在做出最終決策時有人為審查並考量其他因素，則該決策並非「純基於」自動化運用。

[34] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.4 April 2017. European Commission. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Accessed 24 April 2017.
2017年4月4日歐盟執委會29條資料保護工作小組發佈第2016/679號規則關於個資保護影響評估指引（DPIA）以及確認運用是否「可能造成高風險」。http://ec.europa.eu/newsroom/document.cfm?doc_id=44137，瀏覽日期：2017年4月24日。

The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing.

控管者無法透過編造人為參與以規避第22條之規定。例如，若透過人為例行將自動化生成之剖析檔案應用於當事人，而對結果並無任何實際影響，則此仍屬於是純基於自動化運用之決策。

To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data.

為符合有效之人為參與，控管者必須確保對決策之任何監督皆具有意義，而非僅為一種象徵性之行為。該參與應由具有改變決策權限和能力之人執行。參與人應考量所有相關資料，以作為分析之一部分。

As part of their DPIA, the controller should identify and record the degree of any human involvement in the decision-making process and at what stage this takes place.

作為DPIA的一部分，控管者應識別並記錄人為參與決策程序之程度以及其所發生之階段。

B ‘Legal’ or ‘similarly significant’ effects
「法律」或「類似重大」之影響

The GDPR recognises that automated decision-making, including profiling can have serious consequences for individuals. The GDPR does not define ‘legal’ or ‘similarly significant’ however the wording makes it clear that only serious impactful effects will be covered by Article 22.

GDPR認識到自動化決策（包含剖析）可能會對當事人造成嚴重後果。GDPR並無定義何謂「法律」或「類似重大」，然此措辭明確指出第22條僅涵蓋重大之影響。

‘Decision producing legal effects’
「產生法律效果之決策」

A legal effect requires that the decision, which is based on solely automated processing, affects someone’s legal rights, such as the freedom to associate with others, vote in an election, or take legal action. A legal effect may also be something that affects a person’s legal status or their rights under a contract. Examples of this type of effect include automated decisions about an individual

that result in:

法律效果是指基於純自動化運用之決策對某人之合法權利產生影響，例如與他人交流、選舉投票或採取法律行動之自由。其亦可能影響某人之合法地位或於契約下之權利。此類影響之示例包含對當事人之自動化決策導致：

- cancellation of a contract;
  解除契約；
- entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit;
  享有或拒絕法律賦予之特定社會福利之權利，例如子女或住房福利；
- refused admission to a country or denial of citizenship.
  拒絕進入某個國家或拒絕公民身份。

‘Similarly significantly affects him or her’
「對當事人造成類似重大之影響」

Even if a decision-making process does not have an effect on people’s legal rights it could still fall within the scope of Article 22 if it produces an effect that is equivalent or similarly significant in its impact.

即使決策程序並未對當事人之法律權利產生任何效果，然若產生之效果等同於法律效果或有類似重大之影響時，仍屬於第22條之範圍。

In other words, even where there is no change in their legal rights or obligations, the data subject could still be impacted sufficiently to require the protections under this provision. The GDPR introduces the word ‘similarly’ (not present in Article 15 of Directive 95/46/EC) to the phrase ‘significantly affects’. Therefore the threshold for *significance* must be similar to that of a decision producing a legal effect.

易言之，即使其法定權利或義務並無發生變化，當事人仍可因受到重大影響，而需要該條款所提供之保護。GDPR引進「類似」一詞（第95/46 / EC號指令第15條中並無此規定）來修飾「重大影響」。因此，*重大性*之門檻必須類似於產生法律效果之決策。

Recital 71 provides the following typical examples: ‘automatic refusal of an online credit application’ or ‘e-recruiting practices without any human intervention’.

前言第71點提供了以下典型示例：「自動拒絕網路信用申請」或「無人為參與之網路招募活動」。

For data processing to significantly affect someone the effects of the processing must be

sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to:
當資料運用對某人產生重大影響時，運用之效果必須足夠重大或重要到值得引起注意。易言之，決策必須可能：

- significantly affect the circumstances, behaviour or choices of the individuals concerned;
  重大影響相關個人之情況、行為或選擇；
- have a prolonged or permanent impact on the data subject; or
  對當事人產生長期或永久之影響；或
- at its most extreme, lead to the exclusion or discrimination of individuals.
  在極端情況下，造成對個人之排斥或歧視。

It is difficult to be precise about what would be considered sufficiently *significant* to meet the threshold, although the following decisions could fall into this category:
雖然下列決策可能屬於此一類型，但很難準確認定何種情況可被認定為足夠重大以符合門檻：

- decisions that affect someone's financial circumstances, such as their eligibility to credit;
  影響某人財務情況之決策，例如獲得信貸之資格；
- decisions that affect someone's access to health services;
  影響某人獲得醫療服務之決策；
- decisions that deny someone an employment opportunity or put them at a serious disadvantage;
  剝奪某人就業機會或使其處於嚴重劣勢之決策；
- decisions that affect someone's access to education, for example university admissions.
  影響某人接受教育之決策，例如大學錄取。

This bring us also to the issue of online advertising, which increasingly relies on automated tools and involves solely automated individual decision-making. As well as complying with the general provisions of the GDPR, covered in Chapter III, the provisions of the proposed ePrivacy Regulation may also be relevant. Furthermore, children require enhanced protection, as will be discussed below in Chapter V.
此亦顯現了網路廣告的問題，網路廣告越來越依賴於自動化工具，且涉及純自動化之個人決策。除了需遵守第III章所述GDPR之一般規定外，草擬之數位隱私規則之規定亦與此處相關聯。此外，如下文第V章中所述，對兒童需加強保護。

In many typical cases the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile: 'women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items'.
在許多典型情況下，基於剖析而呈現目標式廣告之決策不會對個人造成類似重大影響，例如基於簡單人口統計檔案所為之主流網路時尚商店廣告：「布魯塞爾地區25至35歲女性可能對時尚和某些服飾產品感興趣」。

However it is possible that it may do, depending upon the particular characteristics of the case, including:
然而，依據個案具體特性，廣告可能有類似重大影響，包含：

- the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
  剖析程序之侵入性，包含跨越多個網站、設備和服務追蹤個人；
- the expectations and wishes of the individuals concerned;
  相關個人之期待和願望；
- the way the advert is delivered; or
  廣告之投放方式；或
- using knowledge of the vulnerabilities of the data subjects targeted.
  利用對目標當事人弱點之了解。

Processing that might have little impact on individuals generally may in fact have a significant effect for certain groups of society, such as minority groups or vulnerable adults. For example, someone known or likely to be in financial difficulties who is regularly targeted with adverts for high interest loans may sign up for these offers and potentially incur further debt.
對一般個人影響不大之運用實際上可能對某些社會族群產生重大影響，例如少數族群或易受傷害之成年人。例如，已知或可能陷入財務困境之人經常是高利息貸款廣告的目標，且可能會簽訂這些契約並產生進一步之債務。

Automated decision-making that results in differential pricing based on personal data or personal characteristics could also have a significant effect if, for example, prohibitively high prices effectively bar someone from certain goods or services.
依據個人資料或個人特性造成差別定價之自動化決策亦可能產生重大影響，例如以過高之價格有效地阻止某人取得某些商品或服務。

Similarly significant effects could also be triggered by the actions of individuals other than the

one to which the automated decision relates. An illustration of this is given below.
類似重大影響亦可能並非來自於相關自動化決策而是因個人之行為所觸發。以下示例說明了此種情況。

Example
示例

Hypothetically, a credit card company might reduce a customer's card limit, based not on that customer's own repayment history, but on non-traditional credit criteria, such as an analysis of other customers living in the same area who shop at the same stores.
假設信用卡公司可能並非基於客戶的還款歷史而降低其信用卡之限額，而是基於非傳統的信用標準，例如對居住於同一區域和消費於同一商店之其他客戶的分析。

This could mean that someone is deprived of opportunities based on the actions of others.
此意味著某人可能基於他人之行為而被剝奪了機會。

In a different context using these types of characteristics might have the advantage of extending credit to those without a conventional credit history, who would otherwise have been denied.
在不同脈絡下，使用此類特性之優勢在於可將信用擴展至沒有傳統信用記錄且可能遭受拒絕之人。

C Exceptions from the prohibition
禁止之例外情形

Article 22(1) sets out a general prohibition on solely automated individual decision-making with legal or similarly significant effects, as described above.
如上所述，第22條第1項規定了造成法律或類似重大影響之純自動化個人決策的一般性禁止原則。

This means that the controller should not undertake the processing described in Article 22(1) unless one of the following Article 22(2) exceptions applies - where the decision is:
此意味著控管者不應執行第22條第1項所述之運用，除非適用下列第22條第2項之例外情形－當決策係：

(a) necessary for the performance of or entering into a contract;
履行或簽訂契約所必須；

(b) authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
控管者依歐盟或成員國法律之授權所為，且該法律規定了保護當事人權利和自由以及正當利益之適當安全維護措施；或

(c) based on the data subject's explicit consent.
基於當事人之明確同意。

Where the decision-making involves special categories of data defined in Article 9(1) the controller must also ensure that they can meet the requirements of Article 22(4).
若決策涉及第9條第1項規定之特種資料，則控管者亦須確保能夠滿足第22條第4項之要求。

1. Performance of a contract
履行契約

Controllers may wish to use solely automated decision-making processes for contractual purposes because they believe it is the most appropriate way to achieve the objective. Routine human involvement can sometimes be impractical or impossible due to the sheer quantity of data being processed.
基於契約目的，控管者可能希望使用純自動化決策程序，因其認為此為實現目標最合適之方式。由於運用資料數量龐大，例行的人為參與有時可能是不切實際或不可能的。

The controller must be able to show that this type of processing is necessary, taking into account whether a less privacy-intrusive method could be adopted. [35] If other effective and less intrusive means to achieve the same goal exist, then it would not be 'necessary'.
控管者必須能夠證明此種類型之運用是必要的，同時考量是否得採用較少侵入隱私之方式。[35]若存在可實現相同目的之其他有效且較少侵入性之方式，則該運用就並非係「必要的」。

[35] Buttarelli, Giovanni. Assessing the necessity of measures that limit the fundamental right to the protection of personal data. AToolkit European Data Protection Supervisor, 11 April 2017, https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf Accessed 24 April 2017
Buttarelli，Giovanni。「限制保護個人資料基本權利措施之必要性評估」。歐盟資料保護監管人工具包，2017

Automated decision-making described in Article 22(1) may also be necessary for pre-contractual processing.

第22條第1項所述之自動化決策對於契約簽訂前之(資料)運用亦可能有其必要。

Example

示例

A business advertises an open position. As working for the business in question is popular, the business receives tens of thousands of applications. Due to the exceptionally high volume of applications, the business may find that it is not practically possible to identify fitting candidates without first using fully automated means to sift out irrelevant applications. In this case, automated decision-making may be necessary in order to make a short list of possible candidates, with the intention of entering into a contract with a data subject.

一家企業宣傳一個職位空缺。由於為此企業工作相當受到歡迎，該企業收到了數以萬計的申請表。由於申請表數量異常龐大，企業可能會發現，若無事先使用純自動方式篩選掉不相關之申請表，要確定合適之候選人實際上是不可能的。在此情形下，為列出較短的可能候選人名單，以便與當事人簽訂契約，自動化決策可能是必須的。

Chapter III (Section B) provides more information on contracts as a lawful basis for processing.

第III章（第B節）提供了更多有關以契約作為運用合法依據之資訊。

2. Authorised by Union or Member State law

經歐盟或成員國法律授權

Automated decision-making including profiling could potentially take place under 22(2)(b) if Union or Member State law authorised its use. The relevant law must also lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

若經歐盟或成員國法律授權，自動化決策（包含剖析）可能得依第22條第2項第b款執行。相關法律亦須制定適當措施以維護當事人之權利和自由以及正當利益。

Recital 71 says that this could include the use of automated decision-making defined in Article 22(1) for monitoring and preventing fraud and tax-evasion, or to ensure the security and reliability of a service provided by the controller.

前言第71點指出，這可能包括使用第22條第1項中所定義之自動化決策來監控和防止詐欺及逃稅，或確保控管者所提供服務之安全性和可靠性。

年4月11日，https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf，瀏覽日期：2017年4月24日。

3. Explicit consent
明確之同意

Article 22 requires explicit consent. Processing that falls within the definition of Article 22(1) poses significant data protection risks and a high level of individual control over personal data is therefore deemed appropriate.
第22條要求明確之同意。屬於第22條第1項定義範圍內之運用，具有重大的資料保護風險，因此當事人對其個人資料之高度控制被認為是適當的。

'Explicit consent' is not defined in the GDPR. The WP29 guidelines on consent[36] provide guidance on how this should be interpreted.
GDPR並未定義何謂「明確之同意」。WP29關於同意之指引[36]就如何解釋此一概念提供了指導。

Chapter III (Section B) provides more information on consent generally.
第III章（第B節）提供了有關同意之更多一般資訊。

D. Special categories of personal data – Article 22(4)
特種個人資料 - 第22條第4項

Automated decision-making (described in Article 22(1)) that involves special categories of personal data is only allowed under the following cumulative conditions (Article 22(4)):
涉及特種個人資料之自動化決策（如第22條第1項所述）僅於符合以下累進條件（第22條第4項）時得執行之：

- there is an applicable Article 22(2) exemption; and
  適用第22條第2項之例外情形；及
- point (a) or (g) of Article 9(2) applies.
  適用第9條第2項第a或g款。

> 9(2) (a) - the explicit consent of the data subject; or
> 第9條第2項第a款 － 當事人明確同意；或

[36] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679 WP259. 28 November 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accessed 18 December 2017
29條個資保護工作小組。第2016/679號規則（WP259）關於同意之指引。2017年11月28日，http：//ec.europa.eu/newsroom/just/document.cfm？doc_id = 48499。瀏覽日期：2017年12月18日。

9(2) (g) - processing necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.
第9條第2項第g款 - 基於歐盟或成員國法律為實現重大公共利益所必須之運用，該法律與所追求之目標應符合比例原則、尊重資料保護權之本質、並提供適當和具體之措施，以維護當事人之基本權利和利益。

In both of the above cases, the controller must put in place suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.
在上述兩種情況下，控管者必須採取適當措施以維護當事人之權利和自由以及正當利益。

E Right of data subject[37]
當事人之權利[37]

1. Articles 13(2) (f) and 14(2) (g) - Right to be informed
第 13 條第 2 項第 f 款和 14 條第 2 項第 g 款 － 被告知權

Given the potential risks and interference that profiling caught by Article 22 poses to the rights of data subjects, data controllers should be particularly mindful of their transparency obligations.
鑑於第22條所涉及之剖析對當事人權利構成之潛在風險和干預，資料控管者應特別注意其透明化之義務。

Articles 13(2) (f) and 14(2) (g) require controllers to provide specific, easily accessible information about automated decision-making, based solely on automated processing, including profiling, that produces legal or similarly significant effects.[38]
第13第2項第f款和14條第2項第g款要求控管者就純自動化運用（包含剖析）而為之自動化決策，在造成法律或類似重大影響時，提供明確且易於取得之資訊。[38]

If the controller is making automated decisions as described in Article 22(1), they must:
若控管者執行如第22條第1項所述之自動化決策時，必須：

- tell the data subject that they are engaging in this type of activity;

[37] GDPR Article 12 provides for the modalities applicable for the exercise of the data subject's rights.
GDPR第12條規定了適用於行使當事人權利之方式。
[38] Referred to in Article 22(1) and (4). The WP Guidelines on transparency cover the general information requirements set out in Articles 13 and 14.
於第22條第1項和第4項中提及。WP關於透明化之指引涵蓋了第13條和第14條中規定之一般資訊要求。

告知當事人其正在參與此類活動；

- provide meaningful information about the logic involved; and
  提供有關所涉邏輯之有意義資訊；及
- explain the significance and envisaged consequences of the processing.
  解釋運用之重要性和預設之後果。

Providing this information will also help controllers ensure they are meeting some of the required safeguards referred to in Article 22(3) and Recital 71.
提供這些資訊亦將有助於控管者確保其滿足第22條第3項和前言第71點中提及之某些必要安全維護措施。

If the automated decision-making and profiling does not meet the Article 22(1) definition it is nevertheless good practice to provide the above information. In any event the controller must provide sufficient information to the data subject to make the processing fair,[39] and meet all the other information requirements of Articles 13 and 14.
若自動化決策和剖析不符合第22條第1項之定義，提供上述資訊亦屬一種優良實務做法。無論如何，控管者必須向當事人提供足夠之資訊以確保運用之公正性，[39]並滿足第13條和第14條下所有其他資訊之要求。

Meaningful information about the 'logic involved'
有關「所涉邏輯」之有意義資訊

The growth and complexity of machine-learning can make it challenging to understand how an automated decision-making process or profiling works.
機器學習的成長和複雜性使得理解自動化決策程序或剖析之運作變得具有挑戰性。

The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm.[40] The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.
控管者應以簡單之方式告知當事人背後之基本原理，或達成決策時所依據之標準。GDPR

[39] GDPR Recital 60 "The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore the data subject should be informed of the existence of profiling and the consequences of such profiling."
GDPR 前言第60點「控管者應為當事人提供任何必要之進一步資訊，以確保運用之公正性和透明化，同時考量到運用個人資料之具體情況和背景。此外，應告知當事人剖析之存在以及該剖析之後果。」

要求控管者提供有關所涉邏輯之有意義資訊，但並非是所使用演算法之複雜解釋或完整演算法之揭露。[40]然而，提供之資訊應足夠全面，以使當事人了解所作決策之理由。

Example

示例

A controller uses credit scoring to assess and reject an individual's loan application. The score may have been provided by a credit reference agency, or calculated directly based on information held by the controller.

控管者使用信用評分以評估和拒絕當事人之貸款申請。此評分可能是由信貸諮詢機構提供，或直接依據控管者擁有之資訊加以計算。

Regardless of the source (and information on the source must be provided to the data subject under Article 14 (2) (f) where the personal data have not been obtained from the data subject), if the controller is reliant upon this score it must be able to explain it and the rationale, to the data subject.

無論其來源為何（當個人資料並非由當事人處獲得時，則必須依據第14條第2項第f款向當事人提供有關資料來源之資訊），若控管者依賴此評分，則必須能夠向當事人解釋該評分和其基本理由。

The controller explains that this process helps them make fair and responsible lending decisions. It provides details of the main characteristics considered in reaching the decision, the source of this information and the relevance. This may include, for example:

控管者解釋此程序有助於做出公正和負責任之貸款決策。該控管者提供了在做出決策時所考量主要特徵之詳細資訊、此資訊之來源和關聯性。可能包括，例如：

- the information provided by the data subject on the application form;
  申請表上當事人提供之資訊；
- information about previous account conduct , including any payment arrears; and
  有關先前帳戶行為之資訊，包括任何拖欠付款；及
- official public records information such as fraud record information and insolvency records.

[40] Complexity is no excuse for failing to provide information to the data subject. Recital 58 states that the principle of transparency is "of particular relevance in situations where the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him are being collected, such as in the case of online advertising".

複雜性不得作為無法向當事人提供資訊之理由。前言第58點指出，透明化原則「特別適用於當行為者激增以及活動之技術複雜性使當事人難以知曉和了解與其相關之個人資料是由誰以及以何種目的被蒐集，例如網路廣告」。

官方公開記錄資訊，如詐欺記錄資訊和破產記錄。

The controller also includes information to advise the data subject that the credit scoring methods used are regularly tested to ensure they remain fair, effective and unbiased.
控管者提供之資訊亦包括告知當事人所使用之信用評分方法經定期測試，以確保程序維持公正、有效和無偏見的。

The controller provides contact details for the data subject to request that any declined decision is reconsidered, in line with the provisions of Article 22(3).
依據第22條第3項之規定，控管者提供當事人聯繫細節，以便當事人要求重新考量任何拒絕之決策。

'Significance' and 'envisaged consequences'
「重要性」及「預設之後果」

This term suggests that information must be provided about intended or future processing, and how the automated decision-making might affect the data subject.[41] In order to make this information meaningful and understandable, real, tangible examples of the type of possible effects should be given.
此措辭表明必須提供有關預期或未來運用之資訊，以及自動化決策可能如何影響當事人。[41]為了使這些資訊有意義且可理解，應提供可能影響類型之真實、確切之示例。

In a digital context, controllers might be able to use additional tools to help illustrate such effects.
在數位環境中，控管者也許得使用額外工具以協助說明這些影響。

[41] Council of Europe. Draft Explanatory Report on the modernised version of CoE Convention 108, paragraph 75: "Data subjects should be entitled to know the reasoning underlying the processing of their data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated-decision making including profiling. For instance in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a 'yes' or 'no' decision, and not simply information on the decision itself. Without an understanding of these elements there could be no effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority."
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2 . Accessed 24 April 2017
歐盟理事會。歐盟理事會公約 108 現代化版本之解釋性報告草案第 75 段：「當事人應有權了解運用其資料之原因，包括此種原因之後果，以及從而得出之任何結論，尤其是涉及使用演算法進行自動化決策（包含剖析）之案例。例如，在信用評分之情況下，當事人應有權了解支持相關資料運用以及導致「是」或「否」決策之邏輯，而不僅僅是決策本身之資訊。若不能了解這些要素，則無法有效地行使其他實質的安全維護措施，例如拒絕權及向權責機關提出申訴之權利。」
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2。瀏覽日期：2017 年 4 月 24 日。

Example

示例

An insurance company uses an automated decision making process to set motor insurance premiums based on monitoring customers' driving behaviour. To illustrate the significance and envisaged consequences of the processing it explains that dangerous driving may result in higher insurance payments and provides an app comparing fictional drivers, including one with dangerous driving habits such as fast acceleration and last-minute braking.

一間保險公司使用自動化決策程序，以監控客戶之駕駛行為來設定汽車保險費用。為了說明運用之重要性和預設之後果，該公司解釋了危險駕駛可能導致更高的保險金支付，並提供應用程式可與虛擬之駕駛人相比較，包括一位有危險駕駛習慣，如快速加速和緊急煞車之駕駛人。

It uses graphics to give tips on how to improve these habits and consequently how to lower insurance premiums.

該公司使用圖表以提供有關如何改善這些習慣，以及結果將如何降低保險費之建議。

Controllers can use similar visual techniques to explain how a past decision has been made.

控管者可以使用類似之視覺技術以解釋過去決策如何做成。

2. Article 15(1) (h) - Right of access

第 15 條第 1 項第 h 款 – 近用權

Article 15(1) (h) entitles data subjects to have the same information about solely automated decision- making, including profiling, as required under Articles 13(2) (f) and 14(2) (g), namely:

第15條第1項第h款規定，當事人有權依據第13條第2項第f款和14條第2項第g款之規定，取得有關純自動化決策（包含剖析）之相同資訊，即：

- the existence of automated decision making, including profiling;
  自動化決策（包含剖析）之存在；
- meaningful information about the logic involved; and
  有關所涉邏輯之有意義資訊；及
- the significance and envisaged consequences of such processing for the data subject.
  此類運用對當事人之重要性和預設之後果。

The controller should have already given the data subject this information in line with their Article 13 obligations.[42]

控管者應已經依據第13條之義務向當事人提供了這些資訊。[42]

Article 15(1)(h) says that the controller should provide the data subject with information about the envisaged consequences of the processing, rather than an explanation of a particular decision. Recital 63 clarifies this by stating that every data subject should have the right of access to obtain 'communication' about automatic data processing, including the logic involved, and at least when based on profiling, the consequences of such processing,
第15條第1項第h款規定，控管者應向當事人提供有關運用的預設後果之資訊，而非對特定決策之解釋。前言第63點闡明每位當事人應有近用權以獲得有關自動化資料運用之「溝通」，包括所涉之邏輯，且至少在基於剖析之情況下，此種運用之後果。

By exercising their Article 15 rights, the data subject can become aware of a decision made concerning him or her, including one based on profiling.
透過行使第15條之權利，當事人可了解與其相關之決策，包括基於剖析之決策。

The controller should provide the data subject with general information (notably, on factors taken into account for the decision-making process, and on their respective 'weight' on an aggregate level) which is also useful for him or her to challenge the decision.
控管者應向當事人提供可協助其質疑決策之一般資訊（尤其是關於決策程序中考量之因素，以及總體程度上各個因素所佔之「權重」）。

F. Establishing appropriate safeguards
建立適當安全維護措施

If the basis for processing is 22(2)(a) or 22(2)(c), Article 22(3) requires controllers to implement suitable measures to safeguard data subjects' rights, freedoms and legitimate interests. Under Article 22(2)(b) the Member or Union State law that authorises the processing must also incorporate appropriate safeguarding measures.
若運用係基於第22條第2項第a款或第22條第2項第c款，第22條第3項要求控管者採取適當措施以維護當事人之權利、自由及正當利益。依據第22條第2項第b款，由成員國或歐盟法律授權之運用亦須納入適當之安全維護措施。

Such measures should include as a minimum a way for the data subject to obtain human intervention, express their point of view, and contest the decision.
這些措施應至少包括當事人可取得人為參與、表達其觀點、並對決策提出異議之方式。

[42] GDPR Article 12(3) clarifies the timescales for providing this information.
GDPR第12條第3項闡明了提供此類資訊之時間表。

Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject.
人為參與是一項關鍵要素。任何審核必須由具有適當權限和能力改變決策之人員執行。審核人員應對所有相關資料進行全面性評估，包括當事人所提供之任何其他資訊。

Recital 71 highlights that *in any case* suitable safeguards should also include:
前言第71點強調，*在任何情況下*，適當安全維護措施亦應包括：

> .. specific information to the data subject and the right …… to obtain an explanation of the decision reached after such assessment and to challenge the decision.
> …有關當事人之具體資訊和其權利.....以取得對此類評估所達成決策之解釋，並質疑該決策。

The controller must provide a simple way for the data subject to exercise these rights.
控管者必須為當事人提供一種簡單行使這些權利之方式。

This emphasises the need for transparency about the processing. The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis. Transparency requirements are discussed in Chapter IV (section E).
此處強調了對運用透明化之要求。當事人只有在完全瞭解決策如何做成及其依據為何之基礎上，才能對該決策提出質疑或表達其觀點。透明化之要求在第IV章（第E節）中詳加討論。

Errors or bias in collected or shared data or an error or bias in the automated decision-making process can result in:
蒐集或共享資料中之錯誤或偏差，或自動化決策程序中之錯誤或偏差可能導致：

- incorrect classifications; and
  不正確之分類；及
- assessments based on imprecise projections; that
  基於不精確預測之評估；造成
- impact negatively on individuals.
  對個人負面之影響。

Controllers should carry out frequent assessments on the data sets they process to check for any

bias, and develop ways to address any prejudicial elements, including any over-reliance on correlations. Systems that audit algorithms and regular reviews of the accuracy and relevance of automated decision-making including profiling are other useful measures.
控管者應對其運用之資料集進行經常性評估，以檢驗是否存在偏差，並建立解決任何偏見因素之方法，包括任何對關聯性的過度依賴。其他可用措施包括審核演算法和定期審查自動化決策（包含剖析）之準確性及關聯性的系統。

Controllers should introduce appropriate procedures and measures to prevent errors, inaccuracies[43] or discrimination on the basis of special category data. These measures should be used on a cyclical basis; not only at the design stage, but also continuously, as the profiling is applied to individuals. The outcome of such testing should feed back into the system design.
控管者應使用適當之程序和措施，以防止基於特種類型資料之錯誤、不正確[43]或歧視。這些措施應在周期性基礎上使用；不僅於設計階段，且應在其後剖析應用於個人階段時不間斷地使用。相關測試之結果應向系統設計回饋。

Further examples of appropriate safeguards can be found in the Recommendations section。
有關適當安全維護措施之更多示例，請參閱附錄1「建議」。

V. Children and profiling
兒童和剖析

The GDPR creates additional obligations for data controllers when they are processing children's personal data.
GDPR在運用兒童之個人資料時為資料控管者規範了額外之義務。

Article 22 itself makes no distinction as to whether the processing concerns adults or children. However, recital 71 says that solely automated decision-making, including profiling, with legal or similarly significant effects should not apply to children.[44] Given that this wording is not reflected in the Article itself, WP29 does not consider that this represents an absolute prohibition on this type of processing in relation to children. However, in the light of this recital, WP29

[43] GDPR Recital 71 says that:
GDPR 前言第 71 點表示：
"In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised,…."
「為了確保對當事人之公正和透明化運用，考量到運用個人資料之具體情況和背景，控管者應使用適當之數學或統計程序進行剖析，採行適當技術性和組織性措施，以特別確保改正導致個人資料不正確之因素，並儘量減少錯誤之風險，…」

recommends that, as a rule, controllers should not rely upon the exceptions in Article 22(2) to justify it.

第22條本身並未就運用是否涉及成人或兒童而加以區分。然而，前言第71點表示，具有法律或類似重大影響之純自動化決策（包含剖析）不應適用於兒童。[44]鑑於此一措辭並未反映於該條文本身，WP29並不認為因此絕對禁止此種與兒童相關之運用。然而，依據該前言，WP29建議，作為原則，控管者不應援引第22條第2款中之例外以證明運用之正當性。

There may nevertheless be some circumstances in which it is necessary for controllers to carry out solely automated decision-making, including profiling, with legal or similarly significant effects in relation to children, for example to protect their welfare. If so, the processing may be carried out on the basis of the exceptions in Article 22(2)(a), (b) or (c) as appropriate.

然而，在某些情況下，控管者有必要執行對兒童有法律或類似重大影響之純自動化決策（包含剖析），例如為保護兒童之福祉。若如此，則可依據第22條第2項第a款、第b款或第c款中之例外情形酌情執行運用。

In those cases there must be suitable safeguards in place, as required by Article 22(2)(b) and 22(3), and they must therefore be appropriate for children. The controller must ensure that these safeguards are effective in protecting the rights, freedoms and legitimate interests of the children whose data they are processing.

在這些情況下，須依照第22條第2項第b款和第22條第3項之要求採取適合於兒童之適當安全維護措施。控管者必須確保這些安全維護措施能夠有效地保護資料正被運用的兒童之權利、自由和正當利益。

The need for particular protection for children is reflected in recital 38, which says:

對兒童之特殊保護需求反映於前言第38點中，該前言指出：

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. 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.*
>
> 有鑑於兒童可能未盡知悉其個人資料運用之風險、後果及相關安全維護措施與其權利，兒童就其個人資料應受到特別保護。此種具體保護應適用於兒童個人資料之使用，特別是當該運用之目的係*為行銷、建立個性或用戶剖析檔案，以及當服務直接提供予兒童時蒐集與其相關之個人資料。*

[44] Recital 71 – "such measure should not concern a child".
前言第71點 – 「此類措施不應涉及兒童」。

Article 22 does not prevent controllers from making solely automated decisions about children, if the decision will not have a legal or similarly significant effect on the child. However, solely automated decision making which influences a child's choices and behaviour could potentially have a legal or similarly significant effect on them, depending upon the nature of the choices and behaviours in question.

若決策不會對兒童產生法律或類似重大之影響，第22條並不禁止控管者作出與兒童相關之純自動化決策。然而，影響兒童選擇和行為之純自動化決策是否可能會對其產生法律或類似之重大影響，需具體取決於系爭選擇和行為之性質。

Because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes.[45] Children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising. For example, in online gaming, profiling can be used to target players that the algorithm considers are more likely to spend money on the game as well as providing more personalised adverts. The age and maturity of the child may affect their ability to understand the motivation behind this type of marketing or the consequences.[46]

由於兒童代表了一種較弱勢的社會群體，因此組織通常不應基於行銷目的對其進行剖析。[45]兒童在網絡環境中特別容易受到影響，且更容易受到行為廣告之影響。例如，在網路遊戲中，剖析可用來鎖定演算法所認為更有可能在遊戲上花錢之玩家以及提供更個人化之廣告。兒童的年齡和成熟程度可能會影響其理解此種行銷背後動機或後果之能力。[46]

Article 40(2) (g) explicitly refers to the preparation of codes of conduct incorporating safeguards for children; it may also be possible to develop existing codes.[47]

第40條第2項第g款明確提及制定包含兒童安全維護措施之行為守則；亦可改善現有之守則。[47]

---

[45] The WP29 Opinion 02/2013 on apps on smart devices (WP202), adopted on 27 February 2013, under the specific section 3.10 on Children, specifies at page 26 that "data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, since this will be outside of the scope of the child's understanding and therefore exceed the boundaries of lawful processing".
WP29第02/2013號意見關於智能設備應用程式（WP202），於2013年2月27日通過，關於兒童之具體章節3.10，於第26頁指出「資料控管者不應直接或間接為行為廣告之目的而運用兒童資料，因該運用將不在兒童理解範圍之內，因而超出了合法運用之範圍。」

[46] An EU study on the impact of marketing through social media, online games and mobile applications on children's behaviour found that marketing practices have clear impacts on children's behaviour. This study was based on children aged between 6 and 12 years.
歐盟一項關於透過社群媒體、網路遊戲和手機應用程式對兒童行為影響之研究發現，行銷活動對兒童之行為有明顯的影響。此項研究係針對6至12歲之間的兒童。

[47] One example of a code of conduct dealing with marketing to children is that produced by FEDMA Code of conduct, explanatory memorandum, available at: http://www.oecd.org/sti/ieconomy/2091875.pdf Accessed 15 May 2017. See, in particular: "6.2 Marketers targeting children, or for whom children are likely to constitute a section of their audience, should not exploit children's credulity, loyalty, vulnerability or lack of experience.;

VI. Data protection impact assessments (DPIA) and Data Protection Officer (DPO)
個資保護影響評估（DPIA）和個資保護長（DPO）

Accountability is an important area and an explicit requirement under the GDPR. [48]
課責性是GDPR的一個重要領域且有明確之要求。[48]

As a key accountability tool, a DPIA enables the controller to assess the risks involved in automated decision-making, including profiling. It is a way of showing that suitable measures have been put in place to address those risks and demonstrate compliance with the GDPR.
作為課責性之關鍵工具，DPIA使控管者能夠評估自動化決策（包含剖析）中涉及之風險。DPIA是一種顯示已採取適當措施以因應這些風險並證明已遵守GDPR之方式。

Article 35(3) (a) highlights the need for the controller to carry out a DPIA in the case of:
第35條第3項第a款強調控管者在下列情況執行DPIA之必要性：

> *a systematic and extensive evaluation* of personal aspects relating to natural persons which is *based on* automated processing, *including* profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
> *基於*自動化運用（*包含*剖析）對與自然人相關之個人面向進行*系統性*和*廣泛性*的評估，且基於該評估所作成之決策將對自然人產生法律效果或類似重大影響；

Article 35(3)(a) refers to evaluations including profiling and decisions that are 'based' on automated processing, rather than 'solely' automated processing. We take this to mean that Article 35(3) (a) will apply in the case of decision-making including profiling with legal or similarly significant effects that is *not* wholly automated, as well as solely automated decision-making defined in Article 22(1).
第35條第3項第a款提及之評估包括「基於」自動化運用之剖析和決策，而非「純」自動化運用。我們認為此意味著第35條第3項第a款將適用於有法律或類似重大影響之*非*完全自動

6.8.5 Marketers should not make a child's access to a website contingent on the collection of detailed personal information. In, particular, special incentives such as prize offers and games should not be used to entice children to divulge detailed personal information."
針對兒童行銷行為守則之示例可參考FEDMA行為守則所發行之解釋性備忘錄，請參閱：http：//www.oecd.org/sti/ieconomy/2091875.pdf 瀏覽日期：2017年5月15日。特別參閱：「6.2 針對兒童之行銷人員，或兒童可能構成其部分觀眾之行銷人員，不應利用兒童的易輕信、忠誠、弱勢及缺乏經驗；6.8.5 行銷人員不應將蒐集詳細個人資料作為兒童瀏覽網站之條件。尤其是，不得使用獎品和遊戲等特殊獎勵措施誘使兒童揭露詳細之個人資訊。」

[48] As required by the GDPR Article 5(2).
依據GDPR第5條第2項之要求。

化決策（包含剖析），以及第22條第1項定義之純自動化決策。

If the controller envisages a 'model' where it takes *solely* automated decisions having a *high impact* on individuals based on *profiles* made about them and it *cannot* rely on the individual's consent, on a contract with the individual or on a law authorising this, the controller should not proceed.

若控管者預設一種「模型」，而該模型係基於與個人相關之剖析*檔案*而做出對其產生*高度影響之純自動*化決策，當運用*無法*依賴個人之同意、與個人之契約或法律授權時，則控管者不應繼續該行為。

The controller can still envisage a 'model' of decision-making based on profiling, by significantly increasing the level of human intervention so that the model is *no longer a fully automated decision making process*, although the processing could still present risks to individuals' fundamental rights and freedoms. If so the controller must ensure that they can address these risks and meet the requirements described in Chapter III of these Guidelines.

控管者仍可預設基於剖析之決策「模型」，透過顯著提高人為參與程度，使該模型*不再屬於一種完全自動化的決策程序*，即使此運用仍可能對當事人的基本權利和自由帶來風險 。如是，控管者必須確保其有能力因應這些風險並滿足本指引第III章中所描述之要求。

A DPIA can also be a useful way for the controller to identify what measures they will introduce to address the data protection risks involved with the processing. Such measures[49] could include:

DPIA亦可用於協助控管者識別將採行何種措施以因應運用所涉及之資料保護風險，這些措施[49]可包括：

- informing the data subject about the existence of and the logic involved in the automated decision-making process;
  告知當事人自動化決策程序之存在以及所涉之邏輯；
- explaining the significance and envisaged consequences of the processing for the data subject;
  解釋運用對當事人之重要性和預設之後果；
- providing the data subject with the means to oppose the decision; and
  為當事人提供對決策異議之方式；及
- allowing the data subject to express their point of view.
  允許當事人表達其觀點。

[49] Mirroring the requirements in Article 13(2)(f), Article 14(2)(g) and Article 22(3).
比照第13條第2項第f款、第14條第2項第g款、和第22條第3項之要求。

Other profiling activities may warrant a DPIA, depending upon the specifics of the case. Controllers may wish to consult the WP29 guidelines on DPIAs[50] for further information and to help determine the need to carry out a DPIA.

其他可能需要DPIA之剖析活動將取決於案件之具體情況。控管者可查閱WP29關於DPIA之指引[50]，以獲取更多資訊，並協助確認執行DPIA之必要性。

An additional accountability requirement is the designation of a DPO, where the profiling and/or the automated decision-making is a core activity of the controller and requires regular and systematic monitoring of data subjects on a large scale (Article 37(1)(b).[51]

此外，當剖析和/或自動化決策係控管者之核心業務，且需經常性和系統性地大規模監控當事人時（第37條第1項第b款），額外之課責性要求為指定DPO [51]

[50] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 4 April 2017.. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Accessed 24 April 2017.
29條資料保護工作小組。第2016/679號規則關於個資保護影響評估（DPIA）指引以及確認運用是否「可能造成高風險」。2017年4月4日.. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137。瀏覽日期：2017年4月24日。

[51] Article 29 Data Protection Working Party. Guidelines on Data Protection Officer (DPOs). 5 April 2017; http://ec.europa.eu/newsroom/article29/item-detail.cfm? item_id=612048 Accessed 22 January 2018.
29條資料保護工作小組。個資保護長（DPOs）指引。2017年4月5日;
http://ec.europa.eu/newsroom/article29/item-detail.cfm？item_id = 612048。瀏覽日期：2018年1月22日。

ANNEX 1 - Good practice recommendations
附錄1－ 優良實務做法建議

The following good practice recommendations will assist data controllers in meeting the requirements of the GDPR provisions on profiling and automated decision making.[52]
以下優良實務作法建議將有助於資料控管者符合GDPR關於剖析和自動化決策之規定。[52]

Article 條文	Issue 爭點	Recommendation 建議
5(1)(a),12, 13, 14 第5條第1項第a款、第12條、第13條、第14條	Right to have Information 取得資訊之權利	Controllers should consult the WP29 Guidelines on transparency WP260 for general transparency requirements. 控管者應參考WP29透明化之指引（WP260）關於一般透明化之要求。 In addition to the general requirements, when the controller is processing data as defined in Article 22, they must provide meaningful information about the logic involved. 除一般要求外，當控管者運用第22條定義之資料時，必須提供有關所涉邏輯之有意義資訊。 Instead of providing a complex mathematical explanation about how algorithms or machine-learning work, the controller should consider using clear and comprehensive ways to deliver the information to the data subject, for example: 控管者不需提供有關演算法或機器學習如何作業之複雜數學解釋，而應考量使用清晰且全面性之方式將資訊傳達予當事人，例如： ● the categories of data that have been or will be used in the profiling or decision-making process; 已經或將要於剖析或決策程序中使用之資料類型； ● why these categories are considered pertinent; 為何這些類型被認為係相關的；

[52] Controllers also need to ensure they have robust procedures in place to ensure that they can meet their obligations under Articles 15 – 22 in the timescales provided for by the GDPR.
控管者亦需確保其擁有可靠之程序，以確保能夠在GDPR規定之時間範圍內符合第15-22條規定之義務。

		● how any profile used in the automated decision-making process is built, including any statistics used in the analysis; 如何建構自動化決策程序中所使用之任何剖析檔案，包括分析中使用之任何統計資訊； ● why this profile is relevant to the automated decision-making process; and 為何此類剖析檔案與自動化決策程序相關；及 ● how it is used for a decision concerning the data subject. 如何將其使用於與當事人相關之決策。 Such information will generally be more relevant to the data subject and contribute to the transparency of the processing. 這些資訊通常與當事人更相關，並有助於運用之透明化。 Controllers may wish to consider visualisation and interactive techniques to aid algorithmic transparency[53]. 控管者可能希望考量視覺化和互動式技術以協助演算法之透明化[53]。
6(1)(a) 第6條第1項第a款	Consent as a Basis for processing 以同意作為運用之基礎	If controllers are relying upon consent as a basis for processing they should consult the WP29 Guidelines on consent WP259. 若控管者以同意作為其運用之基礎時，則應參考WP29關於同意之指引（WP259）。
15 第15條	Right of Access 近用權	Controllers may want to consider implementing a mechanism for data subjects to check their profile, including details of the information and sources used to develop it. 控管者可能希望考量實施某種機制使當事人可查閱其剖析檔案，包括建立該剖析檔案之詳細資訊及資料來源。

[53] Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017. Page 87, paragraph 194, March 2017. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf Accessed 24 April 2017
英國資訊委員辦公室 － 大數據、人工智慧、機器學習和資料保護 2.0 版本，03/2017。第 87 頁，第 194 段， 2017 年 3 月. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf 瀏覽日期：2017 年 4 月 24 日。

16 第16條	Right to rectification 更正權	Controllers providing data subjects with access to their profile in connection with their Article 15 rights should allow them the opportunity to update or amend any inaccuracies in the data or profile. This can also help them meet their Article 5(1) (d) obligations. 控管者為當事人提供與其第15條權利相關之剖析檔案近用權，應可使當事人有機會更新或修改資料或剖析檔案中之任何不正確之處。此亦有助於控管者符合第5條第1項第d款之義務。 Controllers could consider introducing online preference management tools such as a privacy dashboard. This gives data subjects the option of managing what is happening to their information across a number of different services – allowing them to alter settings, update their personal details, and review or edit their profile to correct any inaccuracies. 控管者可優先考量使用網路管理工具，例如隱私儀表板。如此可提供當事人管理跨多項不同服務之資訊之選擇 – 允許其更改設置、更新個人詳細資訊、及查看或編輯個人剖析檔案以更正任何不正確之處。
21(1) and (2) 第21條第1項和第2項	Right to object 拒絕權	The right to object in Article 21(1) and (2) has to be explicitly brought to the attention of the data subject and presented clearly and separately from other information (Article 21(4). 必須明確使當事人注意到第21條第1項和第2項之拒絕權，並以清楚並與其他資訊區別之方式呈現（第21條第4項）。 Controllers need to ensure that this right is prominently displayed on their website or in any relevant documentation and not hidden away within any other terms and conditions. 控管者需確保在其網站或任何相關文件中突顯此項權利，且不得隱藏於任何其他條款和條件中。
22 and Recital 71 第22條及	Appropriate safeguards 適當安全維	The following list, though not exhaustive, provides some good practice suggestions for controllers to consider when making solely automated decisions, including profiling (defined in

前言第71點	護措施	Article 22(1)): 以下列表雖非詳盡無遺，但對控管者提供了一些優良實務作法之建議，使其在執行純自動化決策（包含剖析）時得加以考量（定義於第22條第1項）： ● regular quality assurance checks of their systems to make sure that individuals are being treated fairly and not discriminated against, whether on the basis of special categories of personal data or otherwise; 定期對其系統進行品質保證檢查，以確保個人獲得公正待遇且不受到歧視，無論係基於特種類型之個人資料抑或其他資料； ● algorithmic auditing – testing the algorithms used and developed by machine learning systems to prove that they are actually performing as intended, and not producing discriminatory, erroneous or unjustified results; 演算法之稽核 – 測試機器學習系統所使用和研發之演算法，以證明其確實依預設執行，且不產生歧視性、錯誤或不合理之結果； ● for independent 'third party' auditing (where decision-making based on profiling has a high impact on individuals), provide the auditor with all necessary information about how the algorithm or machine learning system works; 對於獨立「第三方」之稽核（當基於剖析之決策對個人有重大影響時），向稽核員提供有關演算法或機器學習系統運作方式之所有必要資訊； ● obtaining contractual assurances for third party algorithms that auditing and testing has been carried out and the algorithm is compliant with agreed standards; 取得第三方演算法之契約保證，確認稽核和測試已被執行，以及演算法符合議定之標準； ● specific measures for data minimisation to incorporate clear

		retention periods for profiles and for any personal data used when creating or applying the profiles; 資料最小化之具體措施，以體現剖析檔案及用於建立或應用剖析檔案時所使用任何個人資料之明確的留存期限； ● using anonymisation or pseudonymisation techniques in the context of profiling; 在剖析背景下使用匿名化或假名化技術； ● ways to allow the data subject to express his or her point of view and contest the decision; and, 允許當事人表達其觀點並對決策提出異議之方式；以及 ● a mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contact point for any queries. 在特定情況下執行人為參與之機制，例如在傳遞自動化決策予當事人時，提供申訴程序之連結、議定之審閱期間及詢問之指定聯絡方式。 Controllers can also explore options such as: 控管者亦可採取以下選項： ● certification mechanisms for processing operations; 運用作業之認證機制； ● codes of conduct for auditing processes involving machine learning; 涉及機器學習之稽核程序行為守則； ● ethical review boards to assess the potential harms and benefits to society of particular applications for profiling. 道德審查委員會，以評估特定剖析應用對社會之潛在危害和益處。

ANNEX 2 – Key GDPR provisions
附錄2－GDPR主要條款

Key GDPR provisions that reference general profiling and automated decision-making
GDPR 中關於一般剖析和自動化決策之主要條款

Article 條文	**Recital** 前言	**Comments** 評論
3(2)(b) 第3條 第2項 第b款	**24** 第24點	The monitoring of data subjects' behaviour as far as their behaviour takes place within the Union. 監控當事人行為，只要其行為發生於歐盟境內。 **Recital 24** **前言第24點** "….tracked on the internet ……use of personal data processing techniques which consist of profiling a natural person, *particularly in order to take decisions* concerning her or him or for analysing or predicting her or his personal preferences, behaviours or attitudes". 「.....在網路上追蹤..... 包含以個人資料運用技術對自然人進行剖析的潛在後續利用，*尤其是為了作成*與其有關的*決策*，或為分析或預測其個人偏好、行為及態度」。
4(4) 第4條 第4項	**30** 第30點	**Article 4(4)** definition of profiling 第4條第4項剖析之定義 **Recital 30** **前言第30點** "online identifiers …., such as Internet Protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags… may leave traces which, in particular when combined with unique identifiers and other information received by the servers, *may be used to create profiles of the natural persons and identify them*." 「網路識別碼.....，例如網際網路協定位址，瀏覽歷程識別碼或其他識別工具例如無線射頻識別標籤...，可能留下足跡，尤其是當與伺服器所接

		收之獨特識別碼及其他資訊相結合時，*可能用於建立與自然人相關之剖析檔案並對其加以識別*。」
5 and 6 第5條及第6條	**72** 第72點	**Recital 72:** **前言第72點：** "Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing **(Article 6)** or data protection principles **(Article 5)**." 「剖析受本法規治理個人資料運用之規則約束，例如運用之法律依據（**第6條**）或資料保護原則（**第5條**）。」
8 第8條	**38** 第38點	Use of children's personal data for profiling. 使用兒童個人資料進行剖析。 **Recital 38:** **前言第38點：** "Children merit specific protection ….. in particular,…to the use of personal data of children for the purposes of….creating personality or user profiles." 「兒童應受特別保護.....尤其是.....為了....建立個性或用戶之剖析檔案，而使用兒童之個人資料。」
13 and 14 第13條及第14條	**60** 第60點	Right to be informed. 被告知權。 **Recital 60:** **前言第60點：** "Furthermore, the data subject shall *be informed of the existence of profiling and the consequences of such profiling* ." 「此外，應*告知當事人剖析之存在以及此類剖析之後果*。」
15 第15條	**63** 第63點	Right of access. 近用權 **Recital 63:** **前言第63點：** "right to know and obtain communication…..with regard to the purposes for

		which the personal data are processed,…..and, *at least* when based on profiling, the consequences of such profiling". 「知情及獲得溝通之權利.....就個人資料運用目的而言，.....且，至少在基於剖析之情況下，此類剖析之後果」。
21(1)(2) and (3) 第21條 第1項 第2項 及 第3項	**70** 第70點	Right to object to profiling. 拒絕剖析之權利 **Recital 70** **前言第70點** "…the right to object to such processing, including profiling to the extent that it is related to such direct marketing." 「…拒絕此類運用之權利，包括與此類行銷相關之剖析。」
23 第23條	**73** 第73點	**Recital 73:** **前言第73點：** "Restrictions concerning specific principles and concerning …….the right to object and decisions based on profiling …….may be imposed by Union or Member State law as far as necessary and proportionate in a democratic society…" to safeguard specific objectives of general public interest. 「關於具體原則之限制和關於.....拒絕權及基於剖析所為決策之限制.....可依據歐盟或成員國法律加以施行，當於民主社會中所必須且符合比例原則時...」為維護一般公眾利益之特定目的。
35(3)(a) 第35條 第3項 第a款	**91** 第91點	A DPIA is required in the case of "a systematic and extensive evaluation of personal aspects relating to natural persons which is *based* on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;" **Covers decision-making including profiling that is not solely automated.** 在「*基於*自動化運用（包含剖析）對與自然人相關之個人面向進行系統性和廣泛之評估，且基於該評估所為之決策造成與自然人相關之法律效果或對該自然人造成類似重大之影響時」，需執行DPIA。**此規定涵蓋包含剖析之非純自動化決策**。

Key GDPR provisions that reference automated decision-making as defined in Article 22

GDPR 中關於第 22 條定義下自動化決策之主要條款

Article 條文	**Recital** 前言	**Comments** 評論
13(2)(f) And **14(2)(g)** 第13條 第2項 第f款 及 第14條 第2項 第g款	**61** 第61點	Right to be informed about: 就以下資訊有被告知之權利：· ● the existence of automated decision-making under **A22(1)** and **(4);** 依據第22條第1項和第4項自動化決策之存在； ● meaningful information about the logic involved; 所涉邏輯之有意義資訊； ● significance and envisaged consequences of such processing. 此類運用之重要性和預設之後果。
15(h) 第15條 第h款		Specific access rights to information about the existence of solely automated decision-making, including profiling. 對純自動化決策（包含剖析）資訊之具體近用權。
22(1) 第22條 第1項	**71** 第71點	Prohibition on decision-making based solely on automated processing, including profiling, which produces legal/similarly significant effects. 禁止會產生法律/或類似重大影響之純自動化運用之決策（包含剖析）。 In addition to the explanation provided in the main body of the guidelines, the following points expand on the rationale for reading Article 22 as a prohibition: 除了本指引主文中提供之解釋外，下列幾點擴大了將第22條作為禁止解釋之理由： ● Although Chapter III is about the rights of the data subject, the provisions in Articles 12 - 22 are not exclusively concerned with the *active* exercise of rights. Some of the rights are *passive*; they do not all

relate to situations where the data subject takes an action i.e. makes a request or a complaint or a demand of some sort. Articles 15-18 and Articles 20-21 are about the data subject actively exercising their rights, but Articles 13 &14 concern duties which the data controller has to fulfil, without any active involvement from the data subject. So the inclusion of Article 22 in that chapter does not in itself mean that it is a right to object;

雖然第III章涉及當事人之權利，但第12-22條之規定並非僅涉及*積極*行使權利。某些權利係*被動的*；這些權利並非皆與當事人採取行動之情況相關，即提出要求或申訴或某種請求。第15-18條和第20-21條係有關當事人積極行使其權利之情況，然第13和14條涉及資料控管者必須履行之義務，而不需當事人任何積極之參與。因此，於該章節中列入第22條並不意味著此係屬於拒絕權；

- Article 12(2) talks about the exercise of ‘data subject rights under Articles 15 to 22; but this does not mean that Article 22(1) itself has to be interpreted as a right. There *is* an active right in A22, but it is part of the safeguards which have to be applied in those cases where automated decision making is allowed (Articles 22(2)(a-c)) - the right to obtain human intervention, express his or her point of view and to contest the decision. It only applies in those cases, because carrying out the processing described in Article 22(1) on other bases is prohibited;

  第12條第2項論及依據第15條至第22條行使「當事人之權利」；然此並不意味著第22條第1項本身必須被解釋為一項權利。第22條中*有*一種積極之權利，然此適用於在允許自動化決策之情況下作為安全維護措施之一部分（第22條第2項第a-c款）－即獲得人為參與、表達觀點和質疑決策之權利。該條款僅適用於這些情況，因在其他基礎上進行第22條第1項所述之運用皆是被禁止的；

- Article 22 is found in a section of the GDPR called “Right to object **and** automated individual decision-making”, implying that Article 22 is *not* a right to object like Article 21. This is further emphasised by the lack in Article 22 of an equivalently explicit information duty as that found in Article 21(4);

  第22條列於於GDPR關於「拒絕權**及**自動化個人決策」之章節中，

此意味著第22條並非屬於第21條下之拒絕權，第22條缺乏與第21條第4項同等明確之資訊義務亦進一步強化此一觀點；

- If Article 22 were to be interpreted as a right to object, the exception in Article 22(2)(c) would not make much sense. The exception states that automated decision-making can still take place if the data subject has given explicit consent (see below). This would be contradictory as a data subject cannot object and consent to the same processing;
  若第22條被解釋為是一種拒絕權，第22條第2項第c款中之例外情形便失去意義。該條之但書規定，若當事人已明確表示同意，則仍可進行自動化決策（請參閱下文）。如此是自相矛盾的，因當事人就同一個運用不得同時拒絕並同意；

- An objection would mean that human intervention must take place. Article 22(2)(a) and (c) exceptions override the main rule in Article 22(1), but only as long as human intervention is available to the data subject, as specified in Article 22(3). Since the data subject (by objecting) has already requested human intervention, Article 22(2)(a) and (c) would automatically be circumvented in every case, thus rendering them meaningless in effect.
  拒絕意味著必須進行人為參與。第22條第2項第a款及第c款規定之例外優先於第22條第1項之主要規定，但只有在依據第22條第3項之規定，當人為參與適用於當事人之情況下才成立。由於當事人（透過拒絕）已要求人為參與，第22條第2項第a款和第c款將在所有情況下自動被規避，從而使其毫無意義。

Recital 71:
前言第71點：

"…Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" …… "*Such measure should not concern a child*"
「...此類運用包含「剖析」，而其係由任何形式之自動化運用個人資料所

		組成，以評估與自然人相關之個人面向，尤其是分析或預測關於當事人於工作中之表現、經濟狀況、健康、個人偏好或興趣、可靠性或行為、所在位置或移動」………「*此類措施不應涉及兒童*」
22(2)(a-c) **第22條第(2)項第a-c款**	**71** **第71點**	**Article 22(2)** lifts the prohibition for processing based on **(a)** the performance of or entering into a contract, **(b)** Union or Member state law, or **(c)** explicit consent. **第22條第2項**基於（**a**）履行或簽訂契約、（**b**）歐盟或成員國法律、或（**c**）明確之同意，可免除對運用之禁止。 **Recital 71** provides further context on **22(2)(b)** and says that processing described in **A22(1):** **前言第71點**提供了關於**第22條第2項第b款**之進一步內容，並指出**第22條第1項**中描述之運用： “should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller…” 「在控管者所適用之歐盟或成員國法律明確授權之情況下，包括依據歐盟機構或國家監管機構之規則、標準和建議而對詐欺和逃稅進行監測和為預防之目的，以及確保控管者所提供服務之安全性和可靠性...」
22(3) **第22項第3款**	**71** **第71點**	**Article 22 (3) and Recital 71** also specify that even in the cases referred to in **22(2)(a)** and **(c)** the processing should be subject to suitable safeguards. 第22條第3項和前言第71點亦規定，即使在第22條第2項第a款和第c款所述之情況下，運用仍應受到適當安全維護措施之保障。 **Recital 71:** **前言第71點:** “which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge

		the decision. Such measure should not concern a child.” 「其中應包含當事人之具體資訊以及獲得人為參與、表達觀點、獲得評估後所作決策之理由、及質疑該決策之權利。此種措施不應涉及兒童。」
23 **第23條**	**73** **第73點**	**Recital 73:** **前言第73點:** “Restrictions concerning specific principles and concerning …….the right to object and decisions based on profiling …….may be imposed by Union or Member State law as far as necessary and proportionate in a democratic society…” to safeguard specific objectives of general public interest. 「關於具體原則之限制和關於.......拒絕權及基於剖析所為決策之限制.......可依據歐盟或成員國法律加以施行，當於民主社會中所必須及符合比例原則時..」為維護一般公共利益之特定目的。
35(3)(a) **第35條** **第3項** **第a款**	**91** **第91點**	Requirement to carry out a DPIA. 執行DPIA之要求。
47(2)(e) **第47條** **第2項** **第e款**		Binding corporate rules referred to in **47(1)** should specify at least “…….the right not to be subject to decisions based solely on automated processing, including profiling in accordance with **Article 22**...” 第47條第1項所述具有約束力之企業守則應至少表明「.......不受純自動化運用所做決策拘束之權利，包含依據第22條執行之剖析...」

ANNEX 3 - Further reading

附錄3 - 延伸閱讀

These Guidelines take account of the following:

本指引參考以下文件：

- WP29 Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted 13 May 2013;
- WP29 Opinion 2/2010 on online behavioural advertising, WP171;
- WP29 Opinion 03/2013 on Purpose limitation, WP 203;
- WP29 Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217
- WP29 Statement on the role of a risk-based approach to data protection legal frameworks, WP218;
- WP29 Opinion 8/2014 on the Recent Developments on the Internet of Things, WP223;
- WP29 Guidelines on Data Protection Officers (DPOs), WP243;
- WP29 Guidelines on identifying a controller or processor's lead supervisory authorityWP244;
- WP29 Guidelines on consent,WP259
- WP29 Guidelines on transparency, WP260
- Council of Europe. Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling;
- Council of Europe. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 01/2017
- Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017
- Office of the Australian Commissioner - Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016
- European Data Protection Supervisor (EDPS) Opinion 7/2015 – Meeting the challenges of big data, 19 November 2015
- Datatilsynet – Big Data – privacy principles under pressure 09/2013
- Council of Europe. Convention for the protection of individuals with regard to automatic processing of personal data - Draft explanatory report on the modernised version of CoE Convention 108, August 2016
- Datatilsynet – The Great Data Race – How commercial utilisation of personal data challenges privacy. Report, November 2015

- European Data Protection Supervisor – Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit
- Joint Committee of the European Supervisory Authorities. Joint Committee Discussion Paper on the use of Big Data by financial institutions 2016-86. https://www.esma.europa.eu/sites/default/files/library/jc-2016 86_discussion_paper_big_data.pdf.
- Commission de la protection de la vie privée. Big Data Rapport https://www.privacycommission.be/sites/privacycommission/files/documents/Big%20Data%20vo or%20MindMap%2022-02-17%20fr.pdf.
- United States Senate, Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, December 18, 2013. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf
- Lilian Edwards & Michael Veale. Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for. Research paper, posted 24 May 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855
- NYTimes.com. Showing the Algorithms behind New York City Services. https://mobile.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city- services.html?referer=https://t.co/6uUVVjOIXx?amp=1. Accessed 24 August 2017
- Council of Europe. Recommendation CM/REC(2018)x of the Committee of Ministers to Member States on Guidelines to promote, protect and fulfil children's rights in the digital environment (revised draft, 25 July 2017). https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren . Accessed 31 August 2017
- Unicef. Privacy, protection of personal information and reputation rights. Discussion paper series: Children's Rights and Business in a Digital World. https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf. Accessed 31 August 2017
- House of Lords. Growing up with the internet. Select Committee on Communications, 2^{nd} Report of Sessions 2016 – 17.

https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm. Accessed 31 August 2017

- Sandra Wachter, Brent Mittelstadt and Luciano Floridi. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, 28 December 2016. https://www.turing.ac.uk/research_projects/data-ethics-group-deg/ . Accessed 13 December 2017
- Sandra Wachter, Brent Mittelstadt and Chris Russell. Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR, 6 October 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289. Accessed 13 December 2017
- Australian Government. Better Practice Guide, Automated Assistance in Administrative Decision- Making. Six steps methodology, plus summary of checklist points Part 7 February 2007. https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf. Accessed 9 January 2018