

「GDPR 相關指引文件研析」委託研究計畫

結案報告

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

中華民國 109 年 9 月

「GDPR 相關指引文件研析」委託研究計畫

結案報告

受託單位：達文西個資暨高科技法律事務所

計畫主持人：葉奇鑫

計畫期程：中華民國 109 年 5 月至 109 年 9 月

研究經費：新臺幣 21 萬元

國家發展委員會 委託研究

中華民國 109 年 9 月

（本報告內容純係作者個人之觀點，不應引申為本機關之意見）

摘要

在 1995 年歐盟「個人資料保護指令」(Directive 95/46/EC) 頒行 21 年後，歐盟於 2016 年 4 月通過「一般資料保護規則」(General Data Protection Regulation, GDPR)，並於 2018 年 5 月 25 日施行。GDPR 強化個人於數位時代的資料保護基本權利，為組織在數位單一市場下的個人資料運用行為提供明確規範，並調和不同會員國個人資料保護法律體系間的分歧。

歐盟依 GDPR 第 68 條設立「歐盟個人資料保護委員會」(European Data Protection Board, EDPB)，其職責包括制定發布 GDPR 條文相關之指引，以利促進 GDPR 在各會員國之一致適用。EDPB 所發布之指引除釐清 GDPR 中核心概念外，也涉及實務界的重要議題。2020 年新冠肺炎 (COVID-19) 疫情爆發，EDPB 連續發布兩份指引文件，力求促進疫情防控與資料保護之雙贏。

我國所面臨的個資保護監理議題，與歐盟有共通之處。且實務中我國公務機關與非公務機關與歐盟之往來與合作，可能亦需遵守 GDPR 之相關規範。因此，有必要進一步瞭解相關指引文件之詳細內容。據此，國家發展委員會挑選 4 份指引文件作為研析標的並將其翻譯為中文，供各界參考。

Abstract

21 years after the adoption of the Data Protection Directive (95/46/EC), the European Union (EU) enacted the General Data Protection Regulation (GDPR), which became effective on 25 May 2018. The GDPR reinforces the fundamental right to protection of personal data in the digital era, provides clear rules on the processing of personal data in the digital single market, while also harmonising the Member States' data protection legal frameworks.

The EU establishes, in accordance with Article 68 of the GDPR, the European Data Protection Board (EDPB), the mandates of which include the issuance of guidelines clarifying the application of the GDPR for purposes of promoting consistent application of the GDPR among the Member States. The guidelines so issued cover not only core concepts of the GDPR, but also issues of practical significance. In response to the COVID-19 pandemic outbreak of 2020, the EDPB has issued two guidelines to ensure the achievement of both pandemic control and data protection.

Given the shared issues of data protection faced by Taiwan and the EU, and the GDPR compliance requirements that may arise during the interaction between Taiwanese and EU organisations, it is necessary to gain further understanding of the relevant guidelines. Against this background, the National Development Council (NDC) has selected 4 guidelines as research subject, and have their full texts translated into Chinese for future reference.

目錄

壹、背景說明.....	1
貳、指引評析.....	3
一、防疫期間接觸史追蹤工具指引（Guidelines 4/2020）	3
（一）指引重要內容.....	3
（二）與我國比較.....	5
二、防疫期間健康資料運用指引（Guidelines 3/2020）	6
（一）指引重要內容.....	6
（二）與我國比較.....	8
三、線上服務運用個人資料指引（Guidelines 2/2019）	9
（一）指引重要內容.....	9
（二）與我國比較.....	11
四、影像裝置運用個人資料指引（Guidelines 3/2019）	13
（一）指引重要內容.....	13
（二）與我國比較.....	14
參、指引翻譯.....	17

壹、背景說明

歐盟於 2016 年 4 月通過「一般資料保護規則」（General Data Protection Regulation，下稱 GDPR），用以取代 1995 年通過之「個人資料保護指令」（Directive 95/46/EC），以求順應科技迅速發展所帶來的資料運用（processing）方式與程度之變革，消弭資料控管者（controller）與資料當事人（data subject）間的權責失衡，同時活絡歐盟內部市場中數位經濟之發展。GDPR 於 2018 年 5 月 25 日施行，在歐盟各會員國境內直接生效。

GDPR 確立歐盟境內一體適用之個資保護法制架構，而其法條規範難免有解釋或適用上的疑義，因此歐盟依 GDPR 第 68 條設立「歐盟個人資料保護委員會」（European Data Protection Board, EDPB），職責包括促進 GDPR 在各會員國之一致適用，並協調各會員國個資保護主管機關之合作。為此目的，EDPB 不時制定發布 GDPR 條文相關之指引、建議或最佳實務做法，闡釋或舉例說明相關條文之具體適用情形，以利資料控管者及受託運用者（processor）遵循。

EDPB 所發布之指引，除釐清 GDPR 中核心概念外，也涉及實務界較具爭議性的重要議題。我國所面臨的個資保護監理議題，與歐盟有共通之處，且實務中我國公務機關與非公務機關與歐盟之往來與合作，可能亦需遵守 GDPR 之相關規範。因此，有必要進一步瞭解相關指引文件之詳細內容。據此，國家發展委員會挑選如下 4 份指引文件作為研析標的並將其翻譯為中文，供各界參考：

1. 關於在新冠肺炎（COVID-19）防疫期間使用位置資料和接觸史追蹤工具之指引 04/2020（以下簡稱「防疫期間接觸史追蹤工具指引」）。
2. 關於在新冠肺炎（COVID-19）防疫期間為科學研究目的運用健康資料之指引 03/2020（以下簡稱「防疫期間健康資料運用指引」）。
3. 關於向當事人提供線上服務時依 GDPR 第 6 條第 1 項第 b 款運用個人資料之指引 2/2019（以下簡稱「線上服務運用個人資料指引」）。
4. 關於以影像裝置運用個人資料之指引 3/2019（以下簡稱「影像裝置運用個人資料指引」）。

貳、指引評析

一、防疫期間接觸史追蹤工具指引（Guidelines 4/2020）

（一）指引重要內容

自 2020 年初以來，新冠肺炎疫情在全球蔓延。歐盟為遏制疫情傳播，運用了諸多技術手段，其中包括使用應用程式追蹤確診者之接觸史、警示曾與確診者接觸之民眾。歐盟會員國公共衛生主管機關組成之 eHealth Network 於 2020 年 4 月提出「歐盟共同工具箱」（Common EU Toolbox）¹，主張以手機應用程式支援接觸史追蹤、協助對抗疫情。

以應用程式記錄民眾曾位於何地、與誰接觸，引發了大規模監控、犧牲隱私之疑慮。對此，EDPB 於 2020 年 4 月 21 日通過本指引，以釐清新冠肺炎防疫期間為評估疫情管控措施之整體成效，或追蹤新冠肺炎患者接觸史之目的，合乎比例地使用位置資料與接觸史追蹤工具之條件與原則。

本指引首先強調，歐盟以 GDPR 和「電子隱私指令」（ePrivacy Directive）²為核心的之資料保護法律框架具有彈性，能夠在有效控制疫情的同時，保護基本人權與自由。歐盟及其會員國的公務機關和其他行動者在遵守資料保護規範的前提下，得將匿名資料或個人資料用於監測並遏制新冠肺炎傳播。

¹ EU eHealth Network, 'Mobile applications to support contact tracing in the EU's fight against COVID-19: Common EU Toolbox for Member States (Version 1.0)' (15 April 2020) <https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf> accessed 22 October 2020.

² Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

位置資料是 GDPR 明確列舉之個人資料。用以模擬病毒傳播並評估管控措施整體成效的位置資料，主要係電子通訊服務與資訊社會服務提供者在提供服務過程中蒐集而得。因此，使用位置資料不僅須符合 GDPR，還應遵守電子隱私指令。如要使用位置資料構建新冠病毒傳播模型，則該資料應予以匿名化，或經當事人明確同意，或符合 GDPR 第 23 條之例外情形。使用位置資料時，應始終以匿名資料為優先選項。資料之匿名化（anonymization）應與假名化（pseudonymisation）區分開來。前者係指移除資料與特定已識別或可得識別的自然人間之連結，使之無法以合理方式識別該自然人，匿名資料因此脫離 GDPR 之適用範圍。而後者並未移除資料與特定自然人間連結，假名資料仍受 GDPR 規範。位置資料難以完全匿名化，因此應特別關注匿名化方法之發展。

接觸史追蹤應用程式是協助控制疫情之有效工具，同時也可能涉及對自然人之系統性、大規模監控，並因此造成對隱私之重大干預。因此，本指引強調，接觸史追蹤應用程式應由個人自願使用，且應尤其注意遵守 GDPR 之資料最小化原則，以及資料保護設計（by design）和預設（by default）要求。資料之運用應依 GDPR 確定其法律依據，資料之留存應符合儲存限制原則。若資料運用涉及高風險（如運用健康資料、實施系統性監控、使用新技術方案等），則須辦理個資保護影響評估（DPIA）。接觸史追蹤應用程式僅可用以支援適格公共衛生人員人工實施之接觸史追蹤，而不得取而代之。

本指引所附「接觸史追蹤應用程式分析指南」附錄，為接觸史追蹤應用程式之開發者與執行者提供一般性指導，以利最大程度地確保透明化，協助接觸史追蹤應用程式為社會接受。該附錄建議接觸史追

蹤應用程式完全自願使用，且在部署此前辦理個資保護影響評估。此類應用程式無需（也不應）使用位置資料，而是應利用使用者的接觸資料（例如行動裝置近距離交換的假名識別碼）。所有資料應儘量儲存於使用者終端，如須使用集中式伺服器，則伺服器運用之資料應限於最小規模。此類應用程式須確保資料安全，特別是須防範伺服器或他人推測個別使用者身分或確診狀況。

（二）與我國比較

位置資料並非我國個人資料保護法（以下簡稱個資法）明文例示之個人資料，但若得與其他資料結合而間接識別特定個人，亦落入個人資料之範疇。因此，為防疫目的而運用位置資料之行為，在我國亦有個資法適用。

按個資法第 15 條、第 16 條本文以及同法第 19 條第 1 項、第 20 條第 1 項本文等規定，公務機關及非公務機關蒐集、處理及利用個人資料應有特定目的，並應分別具備同法第 15 條及第 19 條第 1 項各款合法事由之一（例如經當事人同意）；倘為特定目的外利用，則應分別依同法第 16 條但書及第 20 條第 1 項但書規定辦理。是公務機關或非公務機關如為防疫目的蒐集、處理或利用當事人位置資料，以構建新冠病毒傳播模型、評估新冠肺炎防疫成效或追蹤確診者接觸史，應依上開個資法規定辦理，且應遵守同法第 5 條所揭示之比例原則。

由於位置資料之來源方面，我國與歐盟類似，主要源於電信業者。若由公務機關或非公務機關向電信業者蒐集此等位置資料，於相關之告知義務規定，適用個資法第 9 條「蒐集非由當事人提供之個人資料」所應踐行之告知義務，若符合該條第 2 項規定各款情形之一（例如係公務機關執行法定職務或非公務機關履行法定義務所必要，或基於公

共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人)，則得免除告知義務。

另參照歐盟發布之前揭指引及 GDPR 第 35 條規定，對於新科技之運用方式，在考量該運用之本質、範圍、使用情形及目的後，倘認為該運用可能導致自然人之權利及自由的高風險時，控管者應於運用前，實行該運用對於個資保護之影響評估，此概念於我國個資法第 18 條、第 27 條及同法施行細則第 12 條第 2 項等亦有相似規定，因此倘我國公務機關或非公務機關開發接觸史追蹤應用程式，為增加蒐集、處理及利用個人資料之透明度，亦應考量辦理個資保護影響評估。

二、防疫期間健康資料運用指引（Guidelines 3/2020）

（一）指引重要內容

2020 年初新冠肺炎爆發後，各國紛紛強化醫藥相關研究，力求儘快開發出有效藥物與疫苗，遏制疫情蔓延。藥物與疫苗之研發，需要大量實際數據，其中難免涉及當事人之個人資料，尤其是健康相關之資料。因此，EDPB 於 2020 年 4 月 21 日通過本指引，以釐清新冠肺炎防疫期間運用健康資料實施科學研究所涉及的急迫問題，例如運用之法律依據、當事人權利及其行使方法、相關適當安全維護措施等，以利實現防疫與資料保護之平衡。

本指引首先強調，GDPR 容許在遵循隱私權與個人資料保護制度之前提下，為新冠肺炎防疫相關之科學研究目的運用個人資料。本指引進而分析相關概念與運用之法律依據。GDPR 第 4 條第 15 款定義了

「健康資料」，係指「與健康有關之個人資料，包括揭示其健康狀況之健康照護服務之提供」，此一定義應作廣泛解釋，除包括病歷、醫療檢查結果等正式醫療紀錄外，還包括揭示健康狀況或健康風險之資訊。而所謂「科學研究目的」，亦應做廣泛解釋，包括基礎研究、應用研究和私人資助之研究等。健康資料屬於 GDPR 第 9 條規定的特種個資，其運用須同時具備 GDPR 第 6 條規定的法律依據，以及 GDPR 第 9 條規定的特種個資運用禁止之例外情形。將健康資料用於防疫相關科學研究時，有兩種可能的法律依據：當事人同意，或會員國法律之明文規定。如以當事人同意為依據，須取得當事人自主給予、特定、知情且非模糊，且以聲明或「清楚肯定行為」所為之有效同意；如以會員國法律為依據，則運用之條件與程度依具體法律而有所不同。

接下來，本指引闡明了相關資料保護原則與對當事人權利之限制。考量新冠肺炎防疫期間資料運用之風險，須著重遵守 GDPR 第 5 條規定的透明化、目的限制、資料最小化、儲存限制等原則，並評估是否需要依 GDPR 第 35 條規定辦理個資保護影響評估。原則上，新冠肺炎疫情不會中止或限制當事人依 GDPR 享有之權利。會員國法律如對當事人權利課加限制，其限制應限於必要範圍內。

最後，本指引說明了疫情相關健康資料的境外傳輸規範。新冠肺炎防疫研究之國際合作，可能涉及向歐洲經濟區外傳輸資料。對於資料之國際傳輸，原則上須傳輸至依 GDPR 第 45 條第 3 項取得適足性認定之地區，或採用 GDPR 第 46 條規定之適當安全維護措施（如標準契約條款或有拘束力之企業守則）。若不具備以上情形，在例外情形下，公務機關和私人實體得援用 GDPR 第 49 條之例外條款，例如

第 49 條第 1 項第 d 款（基於公共利益之重要原因所為之必要傳輸）或第 49 條第 1 項第 a 款（明確同意），進行資料之國際傳輸。

（二）與我國比較

我國個資法第 6 條對於病歷、醫療、健康檢查等資料給予特殊保護，原則禁止蒐集、處理和利用。但在此等資料「無從識別」特定當事人之前提下，允許公務機關或學術研究機構為醫療、衛生或犯罪預防之目的而蒐集、處理和利用。此外，法律明文規定或經當事人書面同意者，亦可在特定目的範圍內利用。

從以上條文觀察，我國個資法所規範之健康資料，以病歷、醫療、健康檢查等為限，而不包括正式醫療紀錄以外的健康相關資訊，例如健康應用程式測得之健康數據、當事人自我評估之健康狀況等。其範圍比 GDPR 下「健康資料」較窄。實務上，此一較窄定義的效果是，非屬正式紀錄之健康相關資訊則應依一般個資蒐集、處理或利用之規定辦理。

在暫不考慮健康資料內涵差異的前提下，我國個資法與 GDPR 對於健康資料皆原則禁止運用，且皆將「當事人同意」列作禁止利用之例外情形之一，惟同意之要件不同。依我國個資法第 6 條第 1 項第 6 款，健康資料等特種個資須由當事人「書面」同意，方可蒐集、處理或利用；個資法施行細則第 14 條明定，「書面」同意得以電子文件為之。由此反推可知，蒐集、處理及利用一般個資，其「同意」不以書面為限。相較之下，依 GDPR 運用特種個資與非特種個資，其同意要件並無差別，皆須當事人自主給予、特定、知情且非模糊，且以聲明或「清楚肯定行為」所為之。

更進一步，依我國個資法第 6 條第 2 項，特種個資之「書面同意」與一般個資之「同意」內涵並無不同，惟前者須以書面為之。依我國個資法第 7 條，經當事人同意而蒐集、處理其個資時，係以蒐集者向當事人告知法定事項為前提；於目的外利用時，係以蒐集者向當事人告知利用目的、範圍及不同意之影響為前提。此兩項規範類似 GDPR 中的知情同意要求。第 7 條同時課予蒐集者對取得同意之事實負舉證責任。另將第 7 條同意之規定，連結第 8 條、第 9 條法定告知事項，可推知我國個資法就同意仍須具特定性、非模糊性等內涵。

三、線上服務運用個人資料指引（Guidelines 2/2019）

（一）指引重要內容

線上服務之隱私影響，是現代社會面臨的重要議題之一。針對本質為線上服務之「資訊社會服務」，歐盟以「電子商務指令」（e-Commerce Directive）³確立基本監理架構，並以指令 2015/1535（Directive (EU) 2015/1535）⁴調和會員國之國內監理法規。線上服務之個資運用，則透過 GDPR 加以規範。依據 GDPR，唯有以第 6 條第 1 項第 a 款至第 f 款規定之六項條件為依據時，個資運用方為合法，其中第 b 款為「運用係為履行當事人所立契約所必要，或係締約前應當事人之要求採取步驟所必要」。EDPB 於 2019 年 4 月 9 日通過本指引，並於 2019 年 10 月 8 日通過最新修訂版本，對提供線上服務過程中依

³ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

⁴ Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

GDPR 第 6 條第 1 項第 b 款運用個資之行為提供完整法律分析，並舉例說明相關規範之適用。

本指引首先說明 GDPR 第 6 條第 1 項第 b 款之「履行契約所必要」與同條其他法律依據，特別是第 6 條第 1 項第 a 款之「同意」、第 f 款至「正當利益」之關聯。如控管者擬運用之個人資料事實上係為履行契約所必要，則同意並非適當的法律依據。反之，若運用個資事實上並非為履行契約所必要，則惟有具備其他適當法律依據（如同意或正當利益）時，方得加以運用。簽訂契約並不等同於第 6 條第 1 項第 a 款之「同意」。控管者須在開始運用前即識別適當法律依據，並依其透明化義務告知當事人該法律依據。

第 6 條第 1 項第 b 款涵蓋兩類情形，分別為：個資運用係為履行與當事人間契約所客觀必要，或運用係應當事人之要求採取締約前步驟所客觀必要。本指引在釐清運用「必要性」之含義後，對兩種情形分別討論。「必要性」在歐盟法中有獨立含義，只有無干預性更低的其他可行替代方案時，方為必要。所謂「運用係為履行與當事人間契約所客觀必要」，係指於存在有效契約之前提下，該運用為契約本旨所必要。必要性之判斷與契約條文內容並無必然關聯，契約明文約定允許之運用，未必是履行契約所必要，反之亦然。所謂「運用係應當事人之要求採取締約前步驟所客觀必要」，係指在可能締約的情況下，為遵守當事人提出之請求，而有必要運用個人資料。

本指引亦包含對特定情境下第 6 條第 1 項第 b 款適用性之分析。線上服務契約往往約定為「改進服務」、「線上行為廣告」、「個人化內容」等目的而運用個人資料。大多數情況下，為這些目的而進行的運用活動並非履行契約所必要。若為「防範詐欺」目的而運用資料，

很可能超出履行契約之必要範圍，但控管者可能得援用第 6 條第 1 項第 f 款之正當利益，或第 6 條第 1 項第 c 款之法定義務，作為運用之法律依據。

（二）與我國比較

我國個資法第 19 條第 1 項第 2 款和第 20 條第 1 項本文允許非公務機關在與當事人有契約或類似契約之關係，且已採取適當之安全措施時，為特定目的而蒐集或處理個人資料，並在蒐集之特定目的範圍內利用。而個資法施行細則第 27 條進一步闡明，所謂「契約關係」，包括本約，以及非公務機關與當事人間為履行該契約，所涉及必要第三人之接觸、磋商或聯繫行為及給付或向其為給付之行為。而「類似契約之關係」，則包括契約成立前，為訂約或交易目的進行之磋商或接觸，以及契約無效、撤銷、解除、終止而消滅或履行完成時，非公務機關與當事人為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為。

由前開條文觀之，我國個資法與 GDPR 關於履行契約所涉之個資運用（蒐集、處理和利用），規範邏輯總體一致，皆容許為履行契約、訂約前磋商、契約終止後相關作業等目的而運用個人資料。如欲在契約事務之特定目的必要範圍外，蒐集與契約履行欠缺正當合理關聯之其他個人資料，則須於契約之外，另行取得蒐集之正當事由（如另經當事人同意），始為合法（法務部 106 年 6 月 15 日法律字第 10603503880 號函參照）。又例如我國個資法於基於契約或類似契約關係蒐集、處理或利用個資，亦需結合個資法第 5 條比例原則之規定，以檢視個資運用之必要性。至 GDPR 第 6 條第 1 項第 b 款規定，於檢視個資運用係為履行與當事人間契約所客觀必要，或運用係應當事人

之要求採取締約前步驟所客觀必要時，亦須結合 GDPR 第 5 條第 1 項資料最小化原則，以補充該必要性之評估。

惟我國個資法上履行契約「特定目的之必要範圍」，似不採有如 GDPR 中「必要性」之嚴格解釋（僅以符合有效契約之本旨為限）。法務部法律字第 10603509640 號行政函釋認為，非公務機關使用基於契約或類似契約關係取得之個人資料，對該個人當事人進行行銷，應合乎社會通念下當事人對隱私權之合理期待，故「行銷行為內容」與「契約或類似契約」二者間，應有正當合理之關聯，始符合個資法第 20 條第 1 項本文規定特定目的內利用之範疇，而無需再得「當事人同意」（同條項但書第 6 款）。如行銷與當事人契約或類似契約內容無涉之商品或服務資訊，則除符合個資法第 20 條第 1 項但書第 1 款至第 5 款或第 7 款事由外（例如：為增進公共利益或免除當事人生命、身體、自由、財產上之危險等事由），應依同條項但書第 6 款規定經當事人同意（同意方式請依個資法第 7 條第 2 項規定），始得為之。

以下舉例說明本指引與前開法務部第 10603509640 號函釋立場之區別。設若業者與消費者訂立線上商品買賣契約，並據此取得消費者姓名、電子信箱地址等個人資料，並計劃將此等個資用於行銷目的。依 GDPR 與本指引，行銷通常與線上商品買賣契約本旨無關（縱不實施行銷，亦不妨礙買賣交易之完成），因而非屬「履行契約所必要」。業者如欲將此資料用於行銷，則無論行銷內容與本契約交易是否有合理關聯，皆須於運用前告知當事人運用目的、法律依據等，並取得當事人對行銷運用之有效同意。然依前開法務部函釋，此時是否須另行取得當事人同意，取決於行銷內容與本契約交易之關聯。如所行銷者，

係與本次購買商品相關之商品或服務，則行銷所涉個資利用係基於「契約或類似契約之關係」，無需另行取得當事人同意。

GDPR 與我國個資法皆規定個資運用（蒐集、處理或利用）之不同法律依據。本指引呈現出「為履行契約所必要」與其他法律依據間之關係。控管者須根據運用之目的與情況選擇適當法律依據。當運用「為履行契約所必要」時，「同意」即非適當法律依據。我國個資法主管機關在此方面亦有類似見解。如前開法務部第 10603509640 號函釋認為，如非公務機關與個人資料當事人間具有個資法第 19 條第 1 項第 2 款之關係（契約或類似契約之關係），應優先適用此款，不能再以同條項第 5 款（同意）作為蒐集事由，以避免個資當事人立於不對等地位而無法真正作成自主決定（例如：以同意做為契約成立前提）。GDPR 與我國個資法雖在此一問題上見解相似，但如前開將線上商品買賣取得之個資用於行銷事例所示，由於基於契約運用個資規範的細部差異，實務上結果可能有顯著不同。考量線上服務通常無國界限制，我國業者如向歐盟當事人提供服務，宜以本指引作為最佳實務參考。

四、影像裝置運用個人資料指引（Guidelines 3/2019）

（一）指引重要內容

影像監控裝置之密集使用，以及智慧影像分析技術之普及，對於資料保護有深遠影響。EDPB 於 2019 年 7 月 10 日通過本指引，並於 2020 年 2 月 26 日通過最新修訂版本，為影像監控如何遵循 GDPR 之個資保護規範提供全面指導，並舉例說明相關規範之適用。

本指引首先釐清 GDPR 對於影像監控所涉之個資運用活動之適用性。除落入家庭活動例外、執法指令（EU2016/680）適用範圍等情形

者外，此等個資運用原則上適用 GDPR。運用之法律依據，實務中多為控管者之正當利益、執行符合公共利益之職務或行使公權力所必要。正當利益須為當前真實存在之問題，基於正當利益運用個人資料，須尤其注重與資料當事人間之利益衡平。若實施系統性監控，則僅有在少數情形下得援用當事人同意為法律依據。向第三方揭露影片係對個資的獨立運用，需要具備 GDPR 第 6 條規定的法律依據。

若利用影像監控之影片推斷健康狀況等特種個資，則須同時具有第 6 條運用法律依據，以及第 9 條特種個資運用禁止之例外。影像監控拍攝當事人容貌等身體、生理或行為特徵後，如控管者為「獨特性識別自然人」目的，對其進行技術運用，則構成 GDPR 意義上的運用生物特徵資料 (biometric data)。使用生物特徵資料 (特別是臉部辨識) 將提高當事人權利之風險。為降低風險，須遵守資料最小化原則，並採取一切必要預防措施，保護所運用資料的可用性、完整性與機密性。

控管者以影像監控運用個人資料時，須尤其遵守透明化和資訊提供義務，並保障當事人的近用權、刪除權和拒絕權等權利。根據應向當事人提供之資訊的量，資料控管者得採用層級化方式實現透明化。影像之儲存期間不得超過其運用目的所必要的期間。影像監控所涉個人資料在大部分情況下都應在數天後予以刪除 (自動刪除更佳)。控管者還應採取組織性和技術性措施，維護影像監控所涉個人資料安全。在影像監控可能導致對自然人權利與自由的高風險時，控管者須首先辦理個資保護影響評估。

(二) 與我國比較

我國個資法第 51 條第 1 項第 1 款將「自然人為單純個人或家庭

活動之目的」而蒐集、處理或利用個人資料之行為，排除於該法適用範圍之外。此與 GDPR 第 2 條第 2 項第 c 款的「家庭活動例外」（household exemption）類似。我國實務上，亦有法院參考歐盟法上「家庭活動例外」解釋我國個資法第 51 條第 1 項第 1 款之案例（如臺灣臺北地方法院 107 年度交字第 459 號判決）。本指引對於 GDPR「家庭活動例外」在影像監控方面之適用有較詳盡之舉例說明，或可提供我國個資法主管機關與司法機關日後參考。

我國個資法第 51 條第 1 項第 2 款將「於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料」排除於該法適用範圍之外。因此，於公開場所拍攝資料當事人之照片、影片，如未結合其他個資，則因本條而不受我國個資法規範（臺灣高等法院 107 年度上易字第 893 號判決、臺北高等行政法院 107 年度訴更一字第 27 號判決參照）。至於拍攝影音資料之行為是否侵害資料當事人之其他權益、是否構成違法跟蹤、乃至是否涉嫌妨害秘密罪等，尚需依民法、社會秩序維護法、刑法等其他法律判斷。

公開場所拍攝之影音資料如與其他個資結合，則仍有我國個資法之適用。例如，民眾以包含他人車牌號碼之行車紀錄器影片，向警察機關檢舉違規駕駛行為。由於影片所含車牌號碼得連結車輛登記資料，用以識別拍攝車輛之所有人，故影片攝錄之內容非屬「未與其他個人資料結合之影音資料」，不得援引個資法第 51 條第 1 項第 2 款規定排除個資法之適用。其攝錄與舉發，當依我國個資法第 19 條與第 20 條判斷是否合法（臺中高等行政法院 109 年度交上字第 59 號判決、臺灣臺北地方法院 107 年度交字第 459 號判決參照）。又警察機關對於該行車紀錄器影片之蒐集、處理與利用，亦須遵守我國個資法（法

務部第 10300511510 號函釋參照)。

依 GDPR，影像監控原則上須遵守個資保護規範，除非拍攝之影像不涉及個資運用（亦即，無法直接或間接識別特定個人）。而依我國個資法，對公開場所之攝錄，倘未與其他個人資料結合則不適用個資法。例如公務或非公務機關以行車記錄器所錄存畫面，如僅涉及不特定自然人影像，且未與其他個人資料結合者，尚無個資法之適用(法務部 102 年 3 月 27 日法律字第 10203502790 號書函參照)。對於非公開場所，且非屬自然人為單純個人或家庭活動之目的而實施之影像監控，應有我國個資法之適用。若由公務機關實施者，適用個資法第 15 條及第 16 條規定，例如於該機關執行法定職務之必要範圍，而得蒐集、處理或利用個資。而由非公務機關實施者，如私人公司對其辦公室內部之錄影，適用個資法第 19 條及第 20 條規定，惟個資法之性質為普通法，如其他特別法有相關規定時(例如就業服務法、職業安全衛生法等)，應予優先適用。

參、指引翻譯

詳如後附。

Guidelines



Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak

關於在新冠肺炎（COVID-19）防疫期間使用位置資料和接觸史追蹤工具之指引04/2020

Adopted on 21 April 2020

2020年4月21日通過

Table of contents

目錄

Table of contents 目錄	2
1. Introduction & context 導言與背景	4
2. Use of location data 位置資料之使用	7
2.1 Sources of location data 位置資料之來源	7
2.2 Focus on the use of anonymised location data 聚焦於匿名位置資料之使用	9
3. Contact tracing applications 接觸史追蹤應用程式	13
3.1 General legal analysis 整體法律分析	13
3.2 Recommendations and functional requirements 建議與功能性要求	20
4. Conclusion 結論	23
Annex --Contact Tracing Applications Analysis Guide	25
附錄一接觸史追蹤應用程式分析指南	25

The European Data Protection Board

Having regard to Article 70(1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES:

歐盟個人資料保護委員會

依據歐洲議會與歐盟理事會於2016年4月27日通過之「關於運用*個人資料時對自然人之保護與確保此等資料之自由流通，以及廢除指令95/46/EC的歐盟規則2016/679/EU」（下稱GDPR）第70條第1項第e款；

依據歐洲經濟區聯合委員會於2018年7月6日第154/2018號決定修改之歐洲經濟區（EEA）協議，尤其是附件11及其議定書37¹；

依據「歐盟個人資料保護委員會議事規則」第12條和第22條；

通過以下指引：

* 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」。

¹ References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

本指引所稱之「會員國」應理解為「EEA會員國」。

1. INTRODUCTION & CONTEXT

導言與背景

- 1 Governments and private actors are turning toward the use of data driven solutions as part of the response to the COVID-19 pandemic, raising numerous privacy concerns.

在因應新冠肺炎（COVID-19）疫情全球大流行的過程中，政府與私人行動者逐漸趨向採用資料導向之解決方案，引發了諸多隱私疑慮。

- 2 The EDPB underlines that the data protection legal framework was designed to be flexible and as such, is able to achieve both an efficient response in limiting the pandemic and protecting fundamental human rights and freedoms.

歐盟個人資料保護委員會（EDPB）強調，資料保護法律框架具有彈性，並因此能夠在有效控制疫情的同時，保護基本人權與自由。

- 3 The EDPB firmly believes that, when processing of personal data is necessary for managing the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures. Because the virus knows no borders, it seems preferable to develop a common European approach in response to the current crisis, or at least put in place an interoperable framework.

EDPB堅定地相信，當運用個人資料是管控新冠肺炎疫情的必要舉措時，個人資料保護在建構信任、創造適於接受解決方案的社會環境，並確保這些措施的有效性上，具有不可或缺作用。因為病毒無國界，似宜建構共通性的歐洲模式以因應當前危機，或至少應確立互通框架。

- 4 The EDPB generally considers that data and technology used to help fight COVID-19 should be used to empower, rather than to control, stigmatise, or repress individuals. Furthermore, while data and technology can be important tools, they have intrinsic limitations and can merely leverage the

effectiveness of other public health measures. The general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19.

EDPB原則認為，用於協助對抗新冠肺炎疫情的資料與技術，應用於對個人賦予權能，而非控制、指責或約束個人。此外，雖然資料與技術可能係重要工具，其也有本質上的限制，且僅能對其他公共衛生措施的有效性產生槓桿作用。會員國或歐盟機構所採行的任何涉及運用個人資料對抗新冠肺炎疫情的措施，皆必須以有效性、必要性與合乎比例之基本原則為指導。

- 5 These guidelines clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:

本指引釐清，為下列兩項特定目的，而合乎比例地使用位置資料與接觸史追蹤工具之條件與原則：

- using location data to support the response to the pandemic by modelling the spread of the virus so as to assess the overall effectiveness of confinement measures;

使用位置資料將病毒傳播模型化，評估管控措施（confinement measures）之整體成效，以協助因應疫情；

- contact tracing, which aims to notify individuals of the fact that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus, in order to break the contamination chains as early as possible.

追蹤接觸史以通知相關個人其曾與確診感染病毒者密切接觸，以儘早中斷病毒傳播鏈。

- 6 The efficiency of the contribution of contact tracing applications to the management of the pandemic depends on many factors (e.g., percentage of people who would need to install it; definition of a "contact" in terms of closeness and duration.). Moreover, such applications need to be part of a

comprehensive public health strategy to fight the pandemic, including, inter alia, testing and subsequent manual contact tracing for the purpose of doubt removal. Their deployment should be accompanied by supporting measures to ensure that the information provided to the users is contextualized, and that alerts can be of use to the public health system. Otherwise, these applications might not reach their full impact.

接觸史追蹤應用程式能否有效促進疫情管控，有賴於諸多因素（如安裝該應用程式的人口比例，「接觸」距離與時間的定義）。此外，此等應用程式應作為抗疫全面公共衛生策略的一部分，該全面策略應尤其包括檢驗，以及為消除疑慮而實施之後續人工接觸史追蹤。其部署應配合輔助措施，以確保提供予使用者的資訊符合實際情況，且警示能被公共衛生系統使用。否則此等應用程式可能無法充分發揮其影響。

- 7 The EDPB emphasises that the GDPR and Directive 2002/58/EC (the “ePrivacy Directive”) both contain specific rules allowing for the use of anonymous or personal data to support public authorities and other actors at national and EU levels in monitoring and containing the spread of the SARS-CoV-2 virus².

EDPB強調，GDPR和2002/58/EC號指令（「電子隱私指令」）皆包含明確規定，容許公務機關以及會員國和歐盟層級的其他行動者，使用匿名資料或個人資料監測並遏制新型冠狀病毒（SARS-CoV-2）之傳播²。

- 8 In this regard, the EDPB has already taken position on the fact that the use of contact tracing applications should be voluntary and should not rely on tracing individual movements but rather on proximity information regarding users.³

在此方面，EDPB的立場是，使用接觸史追蹤應用程式應屬自願，不得追蹤個人行動，而是應以使用者的接觸（proximity）資訊為偵測依據³。

² See the [previous statement of the EDPB on the COVID 19 outbreak](#).

見EDPB此前關於新冠肺炎疫情爆發之聲明。

³ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf。

2. USE OF LOCATION DATA

位置資料之使用

2.1 Sources of location data

位置資料之來源

9 There are two principal sources of location data available for modelling the spread of the virus and the overall effectiveness of confinement measures: 用以模擬病毒傳播並評估管控措施整體成效的位置資料，主要來源有二：

- location data collected by electronic communication service providers (such as mobile telecommunication operators) in the course of the provision of their service; and
電子通訊服務提供者（如行動電信營運商）在提供服務過程中蒐集的位置資料；和
- location data collected by information society service providers' applications whose functionality requires the use of such data (e.g., navigation, transportation services, etc.).

資訊社會服務提供者之應用程式，其功能需要使用這些資訊（如導航、交通服務等）。

10 The EDPB recalls that location data⁴ collected from electronic communication providers may only be processed within the remits of articles 6 and 9 of the ePrivacy Directive. This means that these data can only be transmitted to authorities or other third parties if they have been anonymised by the provider or, for data indicating the geographic position of the terminal equipment of a user, which are not traffic data, with the prior consent of the users⁵.

EDPB重申，電子通訊服務提供者所蒐集的位置資料⁴，僅得在電子隱私

⁴ See Art. 2(c) of the ePrivacy Directive.
見電子隱私指令第2條第c項。

指令第6條和第9條容許範圍內運用。這意味著此等資料須經提供者匿名化，或在有關顯示使用者的終端裝置地理位置之資料（非流量資料）的情形，須經使用者事前同意⁵，始得傳輸予公務機關或其他第三方。

- 11 Regarding information, including location data, collected directly from the terminal equipment, art. 5(3) of the “ePrivacy” directive applies. Hence, the storing of information on the user’s device or gaining access to the information already stored is allowed only if (i) the user has given consent⁶ or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the user.

「電子隱私」指令第5條第3項適用於從終端裝置直接蒐集的資訊，包括位置資料。因此，在使用者裝置上儲存資訊，或存取已儲存之資訊，以下列情形為限：（i）使用者給予同意⁶，或（ii）此等儲存和（或）存取對於使用者明確請求之資訊社會服務而言為絕對必要。

- 12 Derogations to the rights and obligations provided for in the “ePrivacy” Directive are however possible pursuant to Art. 15, when they constitute a necessary, appropriate and proportionate measure within a democratic society for certain objectives⁷.

然而，為實現特定目標⁷，在符合民主社會中必要、適當、合乎比例之措施的前提下，得依「電子隱私」指令第15條限縮和豁免該指令規定之權利和義務。

- 13 As for the re-use of location data collected by an information society service provider for modelling purposes (e.g., through the operating

⁵ See Art 6 and 9 of the ePrivacy Directive.

見電子隱私指令第6條和第9條。

⁶ The notion of consent in the ePrivacy directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR

電子隱私指令下同意之含義與GDPR相一致，且須滿足GDPR第4條第11款和第7條之全部要求。

⁷ For the interpretation of article 15 of the “ePrivacy” Directive, see also, CJEU Judgment of 29 January 2008 in case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU.

關於「電子隱私」指令第15條之解釋，參見歐盟法院（CJEU）2008年1月29日第C-275/06號案件，Productores de Música de España (Promusicae) v. Telefónica de España SAU之判決。

system or some previously installed application) additional conditions must be met. Indeed, when data have been collected in compliance with Art. 5(3) of the ePrivacy Directive, they can only be further processed with the additional consent of the data subject or on the basis of a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Art. 23 (1) GDPR.⁸

至於為建模目的（如透過作業系統或某些已安裝的應用程式），對資訊社會服務提供者蒐集的位置資料加以重新使用，須符合其他額外條件。事實上，若資料已經依電子隱私指令第5條第3項蒐集，則其進階運用以下列情形為限：經當事人額外同意；或依歐盟或會員國法律，構成民主社會中為確保GDPR第23條第1項明列之目標，而採取之必要且合乎比例的措施⁸。

2.2 Focus on the use of anonymised location data

聚焦於匿名位置資料之使用

- 14 The EDPB emphasises that when it comes to using location data, preference should always be given to the processing of anonymised data rather than personal data.

EDPB強調，使用位置資料時，應總是優先運用匿名資料，而非個人資料。

- 15 Anonymisation refers to the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable natural person against any “reasonable” effort. This “reasonability test” must take into account both objective aspects (time, technical means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails to pass this

⁸ See section 1.5.3 of the guidelines 1/2020 on processing personal data in the context of connected vehicles.

見「關於聯網汽車相關個人資料運用之指引1/2020」第1.5.3節。

test, then it has not been anonymised and therefore remains in the scope of the GDPR.

匿名化（anonymisation）係指運用技術，移除資料與特定已識別或可得識別的自然人間之連結，使之無法以「合理」（reasonable）方式識別該自然人。此「合理性檢驗」（reasonability test）須同時考量客觀層面因素（時間、技術方法），以及隨具體個案變化之背景因素（包括人口密度、資料的性質與數量之稀有性）。若資料未能通過此檢驗，則其尚未匿名化，因而仍受GDPR規範。

- 16 Evaluating the robustness of anonymisation relies on three criteria: (i) singling-out (isolating an individual in a larger group based on the data); (ii) linkability (linking together two records concerning the same individual); and (iii) inference (deducing, with significant probability, unknown information about an individual).

匿名化之強度有三項評估標準：（i）可區別性（singling-out）（依該資料，將特定個人自群體中分離出來）；（ii）可連結性（linkability）（將關於同一人的兩筆記錄予以連結）；和（iii）可推論性（inference）（極可能推知關於特定個人的未知資訊）。

- 17 The concept of anonymisation is prone to being misunderstood and is often mistaken for pseudonymisation. While anonymisation allows using the data without any restriction, pseudonymised data are still in the scope of the GDPR.

匿名化（anonymization）的概念容易被誤解，且常與假名化（pseudonymisation）混淆。雖然匿名化可使資料之使用不受任何限制，假名資料仍受GDPR規範。

- 18 Many options for effective anonymisation exist⁹, but with a caveat. Data cannot be anonymised on their own, meaning that only datasets as a whole may or may not be made anonymous. In this sense, any intervention on a single data pattern (by means of encryption, or any other mathematical

transformations) can at best be considered a pseudonymisation.

有效的匿名方式甚多⁹，但有一點需要注意。資料自身無法匿名化，換言之，僅得針對資料集整體評估匿名化處理是否可行。因此，（以加密或其他數學轉換方式）對個別資料形式（data pattern）之干預至多屬於假名化處理。

- 19 Anonymisation processes and re-identification attacks are active fields of research. It is crucial for any controller implementing anonymisation solutions to monitor recent developments in this field, especially concerning location data (originating from telecom operators and/or information society services) which are known to be notoriously difficult to anonymise.

匿名化處理與再識別攻擊（re-identification attack）為活躍之研究領域。採取匿名化解決方案之控管者皆應持續關注該領域之最新進展；（來自電信營運商和（或）資訊社會服務的）位置資料以難以匿名化著稱，應特別關注此方面之進展。

- 20 Indeed, a large body of research has shown¹⁰ that *location data thought to be anonymised* may in fact not be. Mobility traces of individuals are inherently highly correlated and unique. Therefore, they can be vulnerable to re-identification attempts under certain circumstances.

事實上，大量研究資料顯示¹⁰，看似已被匿名化的位置資料其實可能並未真正匿名。個人之移動軌跡具有固有的高度關聯性與獨特性，因此在某些情形下容易被再識別。

- 21 A single data pattern tracing the location of an individual over a significant period of time cannot be fully anonymised. This assessment may still hold

⁹ (de Montjoye et al., 2018) "[On the privacy-conscious use of mobile phone data](#)" (de Montjoye et al., 2018) 《論手機資料符合隱私規範之使用》。

¹⁰ (de Montjoye et al., 2013) "[Unique in the Crowd: The privacy bounds of human mobility](#)" and (Pyrgelis et al., 2017) "[Knock Knock, Who's There? Membership Inference on Aggregate Location Data](#)" (de Montjoye et al., 2013) 《群體中的獨特個體：人類移動之隱私邊界》和 (Pyrgelis et al., 2017) 《咚咚咚！誰在門外？以彙總之位置資料推論成員》。

true if the precision of the recorded geographical coordinates is not sufficiently lowered, or if details of the track are removed and even if only the location of places where the data subject stays for substantial amounts of time are retained. This also holds for location data that is poorly aggregated.

在相當時間內持續追蹤個人位置之單一資料形式無法完全被匿名化。若所記錄的地理座標精準度未充分降低，或移除追蹤資料之細節，甚或僅保留當事人長期停留之地點位置，前開結論可能仍會成立。對於未充分彙總之位置資料亦同。

- 22 To achieve anonymisation, location data must be carefully processed in order to meet the reasonability test. In this sense, such a processing includes considering location datasets as a whole, as well as processing data from a reasonably large set of individuals using available robust anonymisation techniques, provided that they are adequately and effectively implemented.

為實現匿名化，須謹慎運用位置資料，以符合「合理性檢驗」。此時，運用包含將位置資料集視為一個整體；以及透過可靠之匿名技術，運用來自相當大規模之群體資料，但以該等技術被適當有效實施為限。

- 23 Lastly, given the complexity of anonymisation processes, transparency regarding the anonymisation methodology is highly encouraged.

最後，因匿名化處理之複雜性，非常鼓勵提升匿名化方法的透明度。

3. CONTACT TRACING APPLICATIONS

接觸史追蹤應用程式

3.1 General legal analysis

整體法律分析

24 The systematic and large scale monitoring of location and/or contacts between natural persons is a grave intrusion into their privacy. It can only be legitimised by relying on a voluntary adoption by the users for each of the respective purposes. This would imply, in particular, that individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all.

對於自然人之位置和（或）接觸進行系統性、大規模監控，係對於隱私之重大干預。僅在使用者因其個別目的自願接受時，始具有正當性。特別地，這意味著個人不得因拒絕使用或無法使用該等應用程式而承受任何不利益。

25 To ensure accountability, the controller of any contact tracing application should be clearly defined. The EDPB considers that the national health authorities could be the controllers¹¹ for such application; other controllers may also be envisaged. In any cases, if the deployment of contact tracing apps involves different actors their roles and responsibilities must be clearly established from the outset and be explained to the users.

為確保課責性，應清楚界定接觸史追蹤應用程式之控管者。EDPB認為，國家衛生主管機關可作為此等應用程式之控管者¹¹，亦可預見存在其他控管者。無論如何，若接觸史追蹤應用程式之部署涉及不同行動者，則自始即應清楚界定其各自角色與責任，並向使用者說明。

26 In addition, with regard to the principle of purpose limitation, the purposes

¹¹ See also European Commission “Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection” Brussels, 16.4.2020 C(2020) 2523 final.

另見歐盟執委會「關於協助對抗新冠肺炎疫情之應用程式資料保護之指導」，布魯塞爾，2020年4月16日，C(2020) 2523 final。

must be specific enough to exclude further processing for purposes unrelated to the management of the COVID- 19 health crisis (e.g., commercial or law enforcement purposes). Once the objective has been clearly defined, it will be necessary to ensure that the use of personal data is adequate, necessary and proportionate.

此外，基於目的限制原則，目的必須足夠具體，以避免為與管理新冠肺炎公衛危機無關之其他目的（如商業或執法目的）進階運用資料。目的一旦被釐清，後續即應確保個人資料之使用係適當、必要且合乎比例。

27 In the context of a contact tracing application, careful consideration should be given to the principle of data minimisation and data protection by design and by default:

對於接觸史追蹤應用程式，應仔細考量資料最小化原則，以及資料保護設計（by design）和預設（by default）要求：

- contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used;

接觸史追蹤應用程式無需追蹤個別使用者之位置，而是應使用接觸資料；

- as contact tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification;

由於接觸史追蹤應用程式得在不直接識別特定個人之情況下運作，應採行適當措施避免再識別；

- the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.

所蒐集之資訊應留存在使用者終端，且相關資料僅在絕對必要時始得蒐集。

28 Regarding the lawfulness of the processing, the EDPB notes that contact tracing applications involve storage and/or access to information already stored in the terminal, which are subject to Art. 5(3) of the “ePrivacy” Directive. If those operations are strictly necessary in order for the provider of the application to provide the service explicitly requested by the user the processing would not require his/her consent. For operations that are not strictly necessary, the provider would need to seek the consent of the user.

關於運用資料之合法性，EDPB注意到，接觸史追蹤應用程式涉及儲存和（或）存取已儲存於終端之資訊，且受「電子隱私」指令第5條第3項規範。應用程式提供者依據使用者之明確請求提供服務的過程中，若此等作業為絕對必要，則運用無須經使用者同意。若此等作業非屬絕對必要，則提供者應徵得使用者同意。

29 Furthermore, the EDPB notes that the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest, i.e. Art. 6(1)(e) GDPR.

此外，EDPB注意到，自願使用接觸史追蹤應用程式之單純事實，並非表示個人資料之運用必須以同意為基礎。若公務機關經法律授權且依法律規定提供服務，則與其運用資料最為相關之法律依據，似乎是為執行符合公共利益之職務所必須，即GDPR第6條第1項第e款之規定。

30 Article 6(3) GDPR clarifies that the basis for the processing referred to in article 6(1)(e) shall be laid down by Union or Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in

the public interest or in the exercise of official authority vested in the controller.¹²

GDPR第6條第3項闡明，GDPR第6條第1項第e款規定之運用依據須由歐盟法或適用於控管者之會員國法律明定。運用之目的應由該法律依據載明；或應為執行符合公共利益之職務或行使控管者已被賦予之公權力所必須（對於第1項第e款規定之運用而言）¹²。

- 31 The legal basis or legislative measure that provides the lawful basis for the use of contact tracing applications should, however, incorporate meaningful safeguards including a reference to the voluntary nature of the application. A clear specification of purpose and explicit limitations concerning the further use of personal data should be included, as well as a clear identification of the controller(s) involved. The categories of data as well as the entities to (and purposes for which, the personal data may be disclosed) should also be identified. Depending on the level of interference, additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing. Finally, the EDPB also recommends including, as soon as practicable, the criteria to determine when the application shall be dismantled and which entity shall be responsible and accountable for making that determination.

然而，作為使用接觸史追蹤應用程式合法基礎之法律依據或立法措施，應納入有實益之安全維護措施，包括敘明該應用程式之自願性質。還應詳述個人資料進階使用之具體目的和明確限制，並明確列舉所涉之控管者。此外，亦應說明資料之類別，以及資料向何實體（和為何等目的）揭露。根據干預之程度，應考量運用之性質、範圍與目的，納入額外安全維護措施。最後，EDPB還建議在可行範圍內，納入停止使用該應用程式之判斷標準，以及負責做此決定並為此負責之實體。

- 32 However, if the data processing is based on another legal basis, such as

¹² See Recital (41).
見前言第41點。

consent (Art. 6(1)(a))¹³ for example, the controller will have to ensure that the strict requirements for such legal basis to be valid are met.

然而，若資料之運用係基於其他法律依據，例如同意（第6條第1項第a款）¹³等法律依據，則控管者須確保嚴格遵守該法律依據之有效條件。

- 33 Moreover, the use of an application to fight the COVID-19 pandemic might lead to the collection of health data (for example the status of an infected person). Processing of such data is allowed when such processing is necessary for reasons of public interest in the area of public health, meeting the conditions of art. 9(2)(i) GDPR¹⁴ or for health care purposes as described in Art. 9(2)(h) GDPR¹⁵. Depending on the legal basis, it might also be based on explicit consent (Art. 9(2)(a) GDPR).

此外，使用應用程式對抗新冠肺炎疫情可能導致蒐集健康資料（如確診者之狀況）。法律允許基於為公共衛生領域的公共利益之必要，並符合GDPR第9條第2項第i款¹⁴；或係依GDPR第9條第2項第h款¹⁵，為健康照護目的所必要時，即可運用此等資料。依具體法律依據，運用此等資料亦可能係基於明示同意（GDPR第9條第2項第a款）。

- 34 In accordance with the initial purpose, Article 9(2)(j) GDPR also allows for health data to be processed when necessary for scientific research purposes or statistical purposes.

依其初始目的，GDPR第9條第2項第j款亦允許為科學研究目的或統計目的之必要而運用健康資料。

¹³ Controllers (especially public authorities) must pay special attention to the fact that consent should not be regarded as freely given if the individual has no genuine choice to refuse or withdraw its consent without detriment.

控管者（特別是公務機關）須尤其注意，若相關個人並無拒絕或撤回其同意而免受不利益之真正選擇，則其同意並非自主給予。

¹⁴ The processing must be based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

運用必須依據歐盟法或會員國法，且該法須規定保障當事人基本權利與自由的適當具體措施，特別是維護職業保密義務之措施。

¹⁵ See Article 9(2)(h) GDPR

見GDPR第9條第2項第h款。

35 The current health crisis should not be used as an opportunity to establish disproportionate data retention mandates. Storage limitation should consider the true needs and the medical relevance (this may include epidemiology-motivated considerations like the incubation period, etc.) and personal data should be kept only for the duration of the COVID-19 crisis. Afterwards, as a general rule, all personal data should be erased or anonymised.

不應藉當前公共衛生危機而不合比例地留存資料。儲存限制應考慮真正需求與醫療關聯度（可能包括潛伏期等流行病學考量要素），且個人資料僅得在新冠肺炎危機存續期間保存。之後，基本原則是，一切個人資料皆應被刪除或匿名化。

36 It is the EDPB's understanding that such apps cannot replace, but only support, manual contact tracing performed by qualified public health personnel, who can sort out whether close contacts are likely to result in virus transmission or not (e.g., when interacting with someone protected by adequate equipment – cashiers, etc. -- or not). The EDPB underlines that procedures and processes including respective algorithms implemented by the contact tracing apps should work under the strict supervision of qualified personnel in order to limit the occurrence of any false positives and negatives. In particular, the task of providing advice on next steps should not be based solely on automated processing.

EDPB認為，此等應用程式僅可支援而不得取代適格公共衛生人員人工實施之接觸史追蹤，由該等公共衛生人員確定密切接觸（如接觸者是否有適當裝備保護，如收銀員等）是否可能導致病毒傳播。EDPB強調，接觸史追蹤應用程式之程序與方法（包括相應演算法），應在適格人員之嚴密監督下執行，以防範發生偽陽性或偽陰性。特別是提供後續措施之建議不得僅基於自動化運用為之。

37 In order to ensure their fairness, accountability and, more broadly, their compliance with the law, algorithms must be auditable and should be

regularly reviewed by independent experts. The application's source code should be made publicly available for the widest possible scrutiny.

為確保公平性、課責性以及更廣意義上之法令遵循性，演算法須可稽核，且應由獨立專家定期審查。為實現儘可能廣泛的監督，應用程式之原始碼應予以公開。

- 38 False positives will always occur to a certain degree. As the identification of an infection risk probably can have a high impact on individuals, such as remaining in self isolation until tested negative, the ability to correct data and/or subsequent analysis results is a necessity. This, of course, should only apply to scenarios and implementations where data is processed and/or stored in a way where such correction is technically feasible and where the adverse effects mentioned above are likely to happen.

一定程度之假陽性是難以避免的。由於感染風險之識別可能對個人有重大影響，如將使其在檢測確認陰性前保持自我隔離，必須具有更正資料和（或）後續分析結果之能力。當然，這僅限依資料之運用和（或）儲存方式，更正在技術上可行，且前開不利影響可能發生之情形。

- 39 Finally the EDPB considers that a data protection impact assessment (DPIA) must be carried out before implementing such tool as the processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution)¹⁶. The EDPB strongly recommends the publication of DPIAs.

最後，EDPB認為，當該項運用被認為是高風險時（健康資料、預期大規模採用、系統性監控、使用新技術方案）¹⁶，在使用此等工具前，須辦理個資保護影響評估（DPIA）。EDPB強烈建議公開個資保護影響評

¹⁶ See WP29 [guidelines \(adopted by the EDPB\) 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](#).

見第29條工作小組（WP29）（由EDPB通過）「[關於第 2016/679號規則（GDPR）中的個資保護影響評估（DPIA）以及確認運用是否「可能造成高風險」之指引](#)」。

估結果。

3.2 Recommendations and functional requirements

建議與功能性要求

- 40 According to the principle of data minimization, among other measures of Data Protection by Design and by Default¹⁷, the data processed should be reduced to the strict minimum. The application should not collect unrelated or not needed information, which may include civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.

依據資料最小化原則，在其他資料保護設計和預設¹⁷的保護措施中，應將所運用的資料嚴格降至最小規模。應用程式不得蒐集無關或不必要之資訊，如婚姻狀況、通訊識別碼（communication identifier）、設備目錄項目（equipment directory item）、訊息、通話記錄、位置資料、裝置識別碼等。

- 41 Data broadcasted by applications must only include some unique and pseudonymous identifiers, generated by and specific to the application. Those identifiers must be renewed regularly, at a frequency compatible with the purpose of containing the spread of the virus, and sufficient to limit the risk of identification and of physical tracking of individuals.

應用程式推播之資料，僅得包含由該應用程式專門生成之特定假名識別碼。識別碼須定期更新，更新頻率應符合控制病毒傳播之需求，且應足以防範識別或實體追蹤特定個人之風險。

- 42 Implementations for contact tracing can follow a centralized or a decentralized approach¹⁸. Both should be considered viable options, provided that adequate security measures are in place, each being accompanied by a set of advantages and disadvantages. Thus, the

¹⁷ See [EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#) 見「[EDPB關於第25條資料保護設計和預設之指引4/2019](#)」。

conceptual phase of app development should always include thorough consideration of both concepts carefully weighing up the respective effects on data protection /privacy and the possible impacts on individuals rights.

接觸史追蹤得以集中式或分散式方式¹⁸進行。在採行適當安全維護措施的前提下，兩種方式皆為可行方案，且各有優勢與缺陷。因此，在應用程式開發構想階段，應對兩種方式均給予充分考量，仔細比較兩者各自對資料保護/隱私之效果，以及對個人權利之可能影響。

- 43 Any server involved in the contact tracing system must only collect the contact history or the pseudonymous identifiers of a user diagnosed as infected as the result of a proper assessment made by health authorities and of a voluntary action of the user. Alternately, the server must keep a list of pseudonymous identifiers of infected users or their contact history only for the time to inform potentially infected users of their exposure, and should not try to identify potentially infected users.

涉及接觸史追蹤系統的所有伺服器所蒐集之接觸史資料和假名識別碼，應以經衛生主管機關審慎評估之確診者自願提供為限。另一方面，伺服器僅得在通知潛在感染者其暴露狀況之必要期間內，保存確診使用者的假名識別碼清單或其接觸史資訊，且不得試圖識別潛在感染者。

- 44 Putting in place a global contact tracing methodology including both applications and manual tracing may require additional information to be processed in some cases. In this context, this additional information should remain on the user terminal and only be processed when strictly necessary and with his prior and specific consent.

構建一套同時使用應用程式及人工追蹤的全球性接觸史追蹤方法，有時可能需要運用額外資訊。這種情形下，該等額外資訊仍應儲存於使用者終端，且其運用應以絕對必要並經使用者事前特定同意為限。

¹⁸ In general, the decentralised solution is more in line with the minimisation principle
一般而言，分散式解決方案更符合資料最小化原則。

- 45 State-of-the-art cryptographic techniques must be implemented to secure the data stored in servers and applications, exchanges between applications and the remote server. Mutual authentication between the application and the server must also be performed.

為保護伺服器 and 應用程式所儲存的資料、確保應用程式與遠端伺服器間資訊交換之安全，應採用最先進的加密技術。應用程式與伺服器間應實施雙向認證（mutual authentication）。

- 46 The reporting of users as COVID-19 infected on the application must be subject to proper authorization, for example through a single-use code tied to a pseudonymous identity of the infected person and linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, no data processing should take place that presumes the validity of the user's status.

在應用程式上通報確診者須有適當授權程序，例如，可使用與確診者假名身分綁定、且與檢疫機構或醫療人員連結之一次性驗證碼。若無法透過安全的方式確認，則不得在推定使用者已確診的基礎上運用資料。

- 47 The controller, in collaboration with the public authorities, have to clearly and explicitly inform about the link to download the official national contact tracing app in order to mitigate the risk that individuals use a third-party app.

與公務機關合作之控管者，應清楚明確地提供國家官方接觸史追蹤應用程式之下載連結，以降低個人使用第三方應用程式之風險。

4. CONCLUSION

結論

48 The world is facing a significant public health crisis that requires strong responses, which will have an impact beyond this emergency. Automated data processing and digital technologies can be key components in the fight against COVID-19. However, one should be wary of the “ratchet effect”. It is our responsibility to ensure that every measure taken in these extraordinary circumstances are necessary, limited in time, of minimal extent and subject to periodic and genuine review as well as to scientific evaluation.

當前全球面臨嚴峻公共衛生危機，需要強而有力的因應方案，而該方案對危機以外的其他事務亦將產生影響。自動化資料運用與數位技術可能是抗擊新冠肺炎之關鍵要素。然而，仍須注意避免「制輪效果」（ratchet effect）。我們有責任確保在此特殊情形下，所採取之各項措施皆確屬必要、有時間限制、範圍最小，且定期進行確實審查與科學評估。

49 The EDPB underlines that one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and moreover data protection principles can play a very important role in the fight against the virus. European data protection law allows for the responsible use of personal data for health management purposes, while also ensuring that individual rights and freedoms are not eroded in the process.

EDPB強調，有效因應當前危機與保障基本權利並非必須選擇其一的選項，而是可以並行之目標；而且，資料保護原則能夠在對抗病毒過程中扮演十分重要之角色。歐洲資料保護法律容許為健康管理目的負責任地使用個人資料，並同時確保此一過程不致侵害個人權利與自由。

For the European Data Protection Board

The Chair

(Andrea Jelinek)

歐盟個人資料保護委員會

主席

(Andrea Jelinek)

ANNEX -- CONTACT TRACING APPLICATIONS ANALYSIS GUIDE

附錄—接觸史追蹤應用程式 分析指南

0. Disclaimer

免責聲明

The following guidance is neither prescriptive nor exhaustive, and its sole purpose of this guide is to provide general guidance to designers and implementers of contact tracing applications. Other solutions than the ones described here can be used and can be lawful as long as they comply with the relevant legal framework (i.e. GDPR and the “ePrivacy” Directive).

下列指導並非規範性文件，亦非對有關事項之窮盡列舉，其唯一目的係對接觸史追蹤應用程式之開發者與執行者提供一般性指導。本指南未論及的其他解決方案亦可供使用，且在符合相關法律框架（即GDPR和電子隱私指令）的前提下，該其他方案亦屬合法。

It must also be noted that this guide is of a general nature. Consequently, the recommendations and obligations contained in this document must not be seen as exhaustive. Any assessment must be carried out on a case-by-case basis, and specific applications may require additional measures not included in this guide.

還應注意，本指南僅提供一般性意見。因此，其所包含之建議與義務並非完全列舉。應針對具體個案進行評估，且特定應用程式可能需採取本指引未明列的其他措施。

1. Summary

摘要

In many Member States stakeholders are considering the use of *contact tracing** applications to help the population discover whether they have

been in contact with a person infected with SARS-Cov-2*.

許多會員國內，利害關係人在考慮運用接觸史追蹤*應用程式協助民眾獲知其是否曾接觸過新型冠狀病毒*的感染者。

The conditions under which such applications would contribute effectively to the management of the pandemic are not yet established. And these conditions would need to be established prior to any implementation of such an app. Yet, it is relevant to provide guidelines bringing relevant information to development teams upstream, so that the protection of personal data can be guaranteed from the early design stage.

目前尚未確立此類應用程式在何條件下始會對疫情之有效控管發揮積極作用。而在使用此類應用程式前，應首先確立這些條件。然而制定指引，提供上游開發團隊相關資訊，將可確保個人資料從初始設計階段即受到保護。

It must be noted that this guide is of a general nature. Consequently, the recommendations and obligations contained in this document must not be seen as exhaustive. Any assessment must be carried out on a case-by-case basis, and specific applications may require additional measures not included in this guide. The purpose of this guide is to provide general guidance to designers and implementers of contact tracing applications.

應注意，本指南僅提供一般性意見。因此，本文件所包含之建議與義務並非完全列舉。應針對具體個案進行評估，且特定應用程式可能需採取本指南未明列的其他措施。本指南旨在為接觸史追蹤應用程式之開發者與執行者提供一般性指導。

Some criteria might go beyond the strict requirements stemming from the data protection framework. They aim at ensuring the highest level of transparency, in order to favour social acceptance of such contact tracing applications.

有些標準可能已超出嚴格意義上資料保護框架的要求。這些標準旨在最大程度地確保透明化，以利此類接觸史追蹤應用程式為社會接受。

To this end, publishers of contact tracing applications should take into account the following criteria:

為此目的，接觸史追蹤應用程式之發布者應考慮下列標準：

- The use of such an application must be strictly voluntary. It may not condition the access to any rights guaranteed by law. Individuals must have full control over their data at all times, and should be able to choose freely to use such an application.

使用此類應用程式應完全基於自願，不得作為取得任何法定權利之條件。個人須始終保有對其資料的完全控制，且應能夠自主選擇使用此類應用程式。

- Contact tracing applications are likely to result in a high risk to the rights and freedoms of natural persons and to require a data protection impact assessment to be conducted prior to their deployment.

接觸史追蹤應用程式可能導致自然人權利與自由的高風險，在部署此等應用程式前，須辦理個資保護影響評估。

- Information on the proximity between users of the application can be obtained without locating them. This kind of application does not need, and, hence, should not involve the use of location data.

無需對應用程式使用者進行定位，即可獲得使用者間密切接觸之資訊。此類應用程式無需，也因此不應，使用位置資料。

- When a user is diagnosed infected with the SARS-Cov-2 virus, only the persons with whom the user has been in close contact within the epidemiologically relevant retention period for contact tracing, should be informed.

若一名使用者被確診感染新型冠狀病毒，所通知之接觸者，應限於在流行病學接觸史追蹤期間（retention period）內曾與確診者密切接觸之人。

- The operation of this type of application might require, depending on the architecture that is chosen, the use of a centralised server. In such a case and in accordance with the principles of data minimisation and data protection by design, the data processed by the centralised server should be limited to the bare minimum:
根據所選擇的架構，此類應用程式之運作可能需要使用集中式伺服器。此時，根據資料最小化以及資料保護設計（by design）之原則，該集中式伺服器所運用之資料應限於最小規模：

- When a user is diagnosed as infected, information regarding its previous close contacts or the identifiers broadcasted by the user's application can be collected, only with the user's agreement. A verification method needs to be established that allows asserting that the person is indeed infected without identifying the user. Technically this could be achieved by alerting contacts only following the intervention of a healthcare professional, for example by using a special one-time code.

當一名使用者被確診後，得蒐集其密切接觸者、或該使用者的應用程式推播之識別碼資訊，但須經該使用者同意。應建立驗證機制，在不識別該使用者的前提下，確認其已被感染。要實現這一驗證，技術面可透過例如特殊一次性驗證碼等方式，且非經醫療人員參與，不得通知接觸者。

- The information stored on the central server should neither allow the controller to identify users diagnosed as infected or having been in contact with those users, nor should it allow the inference of contact patterns not needed for the determination of relevant contacts.

儲存於中央伺服器的資訊不應使控管者識別確診者或接

觸者；在確定相關接觸者的必要範圍外，該等資訊亦不得足以推測接觸模式。

- The operation of this type of application requires to broadcast data that is read by devices of other users and listening to these broadcasts:

此類應用程式之運作需要向其他使用者之裝置推播資料，並接收來自其他使用者的推播。

- It is sufficient to exchange pseudonymous identifiers between users' mobile equipment (computers, tablets, connected watches, etc.), for example by broadcasting them (e.g. via the Bluetooth Low Energy technology).

使用者的行動裝置（電腦、平板電腦、智慧手錶等）間，透過推播（如使用藍牙低功耗（Bluetooth Low Energy）技術）等方式交換假名識別碼即已足夠。

- Identifiers must be generated using state-of-the-art cryptographic processes.

須以最先進的加密程序生成識別碼。

- Identifiers must be renewed on a regular basis to reduce the risk of physical tracking and linkage attacks.

須定期更新識別碼，以降低實體追蹤與連結攻擊（linkage attack）之風險。

- This type of application must be secured to guarantee safe technical processes. In particular:

此類應用程式須確保安全之技術運用。特別是：

- The application should not convey to the users information that allows them to infer the identity or the diagnosis of others. The central server must neither identify users, nor

infer information about them.

應用程式不得向使用者提供足以推測他人身分或診斷狀況的資訊。中央伺服器不得識別使用者，亦不得推測使用者之相關資訊。

Disclaimer: the above principles are related to the claimed purpose of *contact* tracing applications, and to this purpose only, which only aim to automatically inform people potentially exposed to the virus (without having to identify them). The operators of the application and its infrastructure may be controlled by the competent supervisory authority. Following all or part of these guidelines is not necessarily sufficient to ensure a full compliance to the data protection framework.

免責聲明：前開各項原則係關於接觸史追蹤應用程式之目的，且僅與此一目的有關。其旨在自動通知可能已接觸病毒之人（而不識別其身分）。應用程式之作業人員及其基礎設施得受控於權責監管機關。全部或部分遵守本指引，並不必然足以確保完全符合個資保護架構。

2. Definitions

定義

Contact 接觸者	<p>For a contact tracing application, a contact is a user who has participated in an interaction with a user confirmed to be a carrier of the virus, and whose duration and distance induce a risk of significant exposure to the virus infection.</p> <p>對於接觸史追蹤應用程式而言，接觸者係指曾與確診感染病毒之使用者互動，且時間與距離已使其明顯暴露在感染病毒之風險的使用者。</p> <p>Parameters for duration of exposure and distance</p>
-----------------------	--

	<p>between people must be estimated by the health authorities and can be set in the application.</p> <p>暴露時間以及人與人之間的距離標準須由衛生主管機關評估，並得在應用程式中設定。</p>
Location data 位置資料	<p>It refers to all data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a publicly available electronic communications service (as defined in the e-Privacy Directive), as well as data from potential other sources, relating to:</p> <p>係指於電子通訊網路運用或由電子通訊服務所運用，並顯示大眾電子通訊服務（依電子隱私指令之定義）使用者的終端裝置地理位置的一切資料，以及關於下列潛在的其他來源資料：</p> <ul style="list-style-type: none"> • the latitude, longitude or altitude of the terminal equipment; 終端裝置的緯度、經度或高度； • the direction of travel of the user; or 使用者的移動方向；或 • the time the location information was recorded. 記錄位置資訊的時間。
Interaction 互動	<p>In the context of the contact tracing application, an interaction is defined as the exchange of information between two devices located in close proximity to each other (in space and time), within the range of the communication technology used (e.g. Bluetooth). This definition excludes the location of the two users of the interaction.</p>

	<p>對於接觸史追蹤應用程式而言，互動定義為兩裝置間的資訊交換，此兩裝置（在空間與時間方面）位置鄰近，且位於所使用的通訊技術（如藍牙）的作用範圍內。此定義排除2位使用者互動時的位置。</p>
Virus carrier 病毒帶原者	<p>In this document, we consider virus carriers to be users who have been tested positive for the virus and who have received an official diagnosis from physicians or health centres.</p> <p>本文件中，我們認為病毒帶原者係指病毒檢驗呈陽性的使用者，以及已獲醫生或健康中心正式診斷的使用者。</p>
Contact tracing 接觸史追蹤	<p>People who have been in close contact (according to criteria to be defined by epidemiologists) with an individual infected with the virus run a significant risk of also being infected and of infecting others in turn.</p> <p>曾與受病毒感染者（依傳染病學之標準）密切接觸之人，面臨自身被感染及再感染他人之高度風險。</p> <p>Contact tracing is a disease control methodology that lists all people who have been in close proximity to a carrier of the virus so as to check whether they are at risk of infection and take the appropriate sanitary measures towards them.</p> <p>接觸史追蹤係一疾病管控方法，其列出曾與病毒帶原者密切接觸之全部人員，查驗其是否有感染風險，並對其採取適當衛生管理措施。</p>

3. General

總則

GEN-1	<p>The application must be a complementary tool to traditional contact tracing techniques (notably interviews with infected persons), i.e. be part of a wider public health program. It must be used <u>only</u> up until the point manual contact tracing techniques can manage alone the amount of new infections.</p> <p>該應用程式須作為傳統接觸史追蹤技術（以感染者訪談為主）之輔助工具，亦即，其應作為更廣泛的公共衛生方案之一部分。人工接觸史追蹤技術足以單獨管理新增感染者時，即應<u>停止</u>使用該應用程式。</p>
GEN-2	<p>At the latest when “return to normal” is decided by the competent public authorities, a procedure must be put in place to stop the collection of identifiers (global deactivation of the application, instructions to uninstall the application, automatic uninstallation, etc.) and to activate the deletion of all collected data from all databases (mobile applications and servers).</p> <p>至遲於主管公務機關決定「恢復常態」時，應落實相關程序，以停止蒐集識別碼（總體的停用該應用程式、指示解除安裝該應用程式、自動解除安裝等），並將所蒐集之資料自全部資料庫（行動應用程式與伺服器）中刪除。</p>
GEN-3	<p>The source code of the application and of its backend must be open, and the technical specifications must be made public, so that any concerned party can audit the code, and where relevant - contribute to improving the code, correcting possible bugs and ensuring transparency in the processing of personal data.</p> <p>應用程式及其後端之原始碼須開放，且其技術規格須予以公開，以利相關各方稽核該代碼，在可行範圍內協助改進代</p>

	碼，糾正可能存在的錯誤，並確保個人資料運用的透明性。
GEN-4	<p>The stages of deployment of the application must make it possible to progressively validate its effectiveness from a public health point of view. An evaluation protocol, specifying indicators allowing to measure the effectiveness of the application, must be defined upstream for this purpose.</p> <p>部署應用程式之各個階段須能夠在公共衛生的觀點上逐步驗證該程式的有效性。為此目的，須在上游定義評估方案，載明衡量該應用程式有效性的指標。</p>

4. Purposes

目的

PUR-1	<p>The application must pursue the sole purpose of contact tracing so that people potentially exposed to the SARS-Cov-2 virus can be alerted and taken care of. It must not be used for another purpose.</p> <p>應用程式之唯一目的，應係追蹤接觸史，使可能暴露在新型冠狀病毒之人員獲得警示與適當照護，不得用於其他目的。</p>
PUR-2	<p>The application must not be diverted from its primary use for the purpose of monitoring compliance with quarantine or confinement measures and/or social distancing.</p> <p>應用程式不得為了監督使用者是否遵守隔離或管控措施，和（或）社交距離而偏離其主要用途。</p>
PUR-3	The application must not be used to draw conclusions on the

	<p>location of the users based on their interaction and/or any other means.</p> <p>應用程式不得基於使用者的互動，和（或）以其他方式，判斷使用者的位置。</p>
--	---

5. Functional considerations

功能性考量

FUNC-1	<p>The application must provide a functionality enabling users to be informed that they have been potentially exposed to the virus, this information being based on proximity to an infected user within a window of X days prior to the positive screening test (the X value being defined by the health authorities).</p> <p>應用程式必須包含通知使用者其可能曾暴露在病毒中之功能，該資訊是以在確診的使用者檢驗呈陽性前的X天內與其近距離接觸程度為基準（X之數值由衛生主管機關定義）。</p>
FUNC-2	<p>The application should provide recommendations to users identified as having being potentially exposed to the virus. It should relay instructions regarding the measures they should follow, and they should allow the user to request advises. In such cases, a human intervention would be mandatory.</p> <p>應用程式應向被認定可能暴露在病毒中的使用者提供建議。其應向使用者轉達所應遵守的措施，並應允許使用者尋求建議。此時，必須有人為參與。</p>
FUNC-3	<p>The algorithm measuring the risk of infection by taking into account factors of distance and time and thus determining when a contact has to be recorded in the contact tracing list, must be securely tuneable to take into account the most recent</p>

	<p>knowledge on the spread of the virus.</p> <p>考量距離與時間要素，並據以判斷特定接觸者是否應被納入接觸史追蹤名單之評估感染風險的演算法，須可安全地加以調整，以便將關於病毒傳播的最新發現納入考量。</p>
FUNC-4	<p>Users must be informed in case they have been exposed to the virus, or must regularly obtain information on whether or not they have been exposed to the virus, within the incubation period of the virus.</p> <p>使用者必須在曾暴露於病毒後獲得通知，或定期獲得其是否曾在病毒潛伏期內暴露於病毒中之資訊。</p>
FUNC-5	<p>The application should be interoperable with other applications developed across EU Member States, so that users travelling across different Member States can be efficiently notified.</p> <p>應用程式與歐盟會員國開發的其他應用程式應有互通性，以便行經不同會員國的使用者即時獲得通知。</p>

6. Data

資料

DATA-1	<p>The application must be able to broadcast and receive data via proximity communication technologies like Bluetooth Low Energy so that contact tracing can be carried out.</p> <p>應用程式須能夠通過藍牙低功耗等鄰近通訊（proximity communication）技術推播並接收資料，以實施接觸史追蹤。</p>
DATA-2	<p>This broadcast data must include cryptographically strong pseudo-random identifiers, generated by and specific to the application.</p>

	<p>推播資料必須包含高強度加密隨機假名識別碼，該識別碼由該應用程式生成，且為該應用程式獨有。</p>
DATA-3	<p>The risk of collision between pseudo-random identifiers should be sufficiently low.</p> <p>隨機假名識別碼間的重複機率應足夠低。</p>
DATA-4	<p>Pseudo-random identifiers must be renewed regularly, at a frequency sufficient to limit the risk of re-identification, physical tracking or linkage of individuals, by anyone including central server operators, other application users or malicious third parties. These identifiers must be generated by the user's application, possibly based on a seed provided by the central server.</p> <p>隨機假名識別碼應定期更新，更新頻率應足以限制任何人（包括中央伺服器作業人員、其他應用程式使用者或惡意第三方）再識別、實體追蹤或連結特定個人之風險。此等識別碼須由使用者的應用程式生成，其可以中央伺服器提供的初始值（seed）為基礎。</p>
DATA-5	<p>According to the data minimisation principle, the application must not collect data other than what is strictly necessary for the purpose of contact tracing</p> <p>根據資料最小化原則，應用程式不得在接觸史追蹤目的之嚴格必要範圍外，蒐集其他資料。</p>
DATA-6	<p>The application must not collect location data for the purpose of contact tracing. Location data can be processed for the sole purpose of allowing the application to interact with similar applications in other countries and should be limited in precision to what is strictly necessary for this sole purpose.</p> <p>應用程式不得為接觸史追蹤目的蒐集位置資料。位置資料之運用，應以允許該應用程式與其他國家的類似應用程式互動</p>

	為唯一目的，且應限於實現此唯一目的之嚴格必要範圍內。
DATA-7	<p>The application should not collect health data in addition to those that are strictly necessary for the purposes of the app, except on an optional basis and for the sole purpose of assisting in the decision making process of informing the user.</p> <p>應用程式不得在其目的之嚴格必要範圍外蒐集健康資料，但基於其自行選擇及專為協助通知使用者決策過程之目的則不在此限。</p>
DATA-8	<p>Users must be informed of all personal data that will be collected. This data should be collected only with the user authorization.</p> <p>蒐集一切個人資料，均應告知使用者。蒐集資料須經使用者授權。</p>

7. Technical properties

技術屬性

TECH-1	<p>The application should available technologies such as use proximity communication technology (e.g. Bluetooth Low Energy) to detect users in the vicinity of the device running the application.</p> <p>應用程式應使用鄰近通訊技術（如藍牙低功耗），偵測運行該應用程式之裝置附近的使用者。</p>
TECH-2	<p>The application should keep the history of a user's contacts in the equipment, for a predefined limited period of time.</p> <p>應用程式應將使用者的接觸史記錄保存在設備上，保存期限應預先設定。</p>

TECH-3	<p>The application may rely on a central server to implement some of its functionalities.</p> <p>應用程式得透過中央伺服器執行部分功能。</p>
TECH-4	<p>The application must be based on an architecture relying as much as possible on users' devices.</p> <p>應用程式之基礎架構必須儘可能地依賴使用者的裝置。</p>
TECH-5	<p>At the initiative of users reported as infected by the virus and after confirmation of their status by an appropriately certified health professional, their contact history or their own identifiers should be transmitted to the central server.</p> <p>使用者主動通報其被病毒感染，且其狀態經適格醫療人員確認後，其接觸史或其自身識別碼應被傳輸至中央伺服器。</p>

8. Security

安全

SEC-1	<p>A mechanism must verify the status of users who report as SARS-CoV-2 positive in the application, for example by providing a single-use code linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, data must not be processed.</p> <p>經應用程式通報為新冠病毒陽性，必須有相關機制確認使用者之狀態，例如，可提供與檢疫機構或醫療人員連結之一次性驗證碼。若無法安全地獲得確認，則不得運用資料。</p>
SEC-2	<p>The data sent to the central server must be transmitted over a secure channel. The use of notification services provided by OS platform providers should be carefully assessed, and should not lead to disclosing any data to third parties.</p>

	<p>必須以安全方式向中央伺服器傳輸資料。若要使用作業系統提供者提供的通知服務，須進行審慎評估，且不得因此向第三方揭露任何資料。</p>
SEC-3	<p>Requests must not be vulnerable to tampering by a malicious user</p> <p>不得讓惡意使用者輕易竄改請求。</p>
SEC-4	<p>State-of-the-art cryptographic techniques must be implemented to secure exchanges between the application and the server and between applications and as a general rule to protect the information stored in the applications and on the server. Examples of techniques that can be used include for example : symmetric and asymmetric encryption, hash functions, private membership test, private set intersection, Bloom filters, private information retrieval, homomorphic encryption, etc.</p> <p>為確保應用程式與伺服器間、應用程式間之資訊交換安全，且作為保護伺服器和應用程式所儲存資料的一般原則，應採用最先進的加密技術。可採用的技術示例包括：對稱及不對稱加密、雜湊函數（hash function）、私人成員檢驗（private membership test）、隱私保護集合交集（private set intersection）、布隆過濾器（Bloom filter）、私有資訊擷取（private information retrieval）、同態加密（homomorphic encryption）等。</p>
SEC-5	<p>The central server must not keep network connection identifiers (e.g., IP addresses) of any users including those who have been positively diagnosed and who transmitted their contacts history or their own identifiers.</p> <p>中央伺服器不得保存任何使用者的網路連結識別碼（如IP位址），對於曾經診斷為陽性、已傳輸其接觸史或其自身識別碼的使用者亦同。</p>

SEC-6	<p>In order to avoid impersonation or the creation of fake users, the server must authenticate the application.</p> <p>為防範冒名行為或創設使用者假身分，伺服器必須認證應用程式。</p>
SEC-7	<p>The application must authenticate the central server.</p> <p>應用程式必須對中央伺服器進行認證。</p>
SEC-8	<p>The server functionalities should be protected from replay attacks.</p> <p>應保護伺服器功能免受重送攻擊（replay attack）。</p>
SEC-9	<p>The information transmitted by the central server must be signed in order to authenticate its origin and integrity.</p> <p>中央伺服器傳輸之資訊須經數位簽名，以認證其來源與完整性。</p>
SEC-10	<p>Access to all data stored in the central server and not publicly available must be restricted to authorised persons only.</p> <p>一切儲存於中央伺服器或不公開之資料，僅限業經授權之人存取。</p>
SEC-11	<p>The device's permission manager at the operating system level must only request the permissions necessary to access and use when necessary the communication modules, to store the data in the terminal, and to exchange information with the central server.</p> <p>裝置作業系統層面的權限管理器發出之請求，其目的應限於在必要時存取和使用通訊模組、在終端儲存資料，以及與中央伺服器交換資訊。</p>

9. Protection of personal data and privacy of natural persons

保護自然人個人資料與隱私

Reminder: the following guidelines concern an application whose sole purpose is contact tracing.

注意：下列指引係針對專為接觸史追蹤為目的之應用程式

PRIV-1	Data exchanges must be respectful of the users' privacy (and notably respect the principle of data minimisation). 資料交換須尊重使用者之隱私（尤其應遵守資料最小化原則）。
PRIV-2	The application must not allow users to be directly identified when using the application. 使用者使用該應用程式時，不得被直接識別。
PRIV-3	The application must not allow users' movements to be traced. 應用程式不得讓使用者之行動被追蹤。
PRIV-4	The use of the application should not allow users to learn anything about other users (and notably whether they are virus carriers or not). 不得讓使用者因使用該應用程式獲知其他使用者的資訊（特別是其他使用者是否為病毒帶原者）。
PRIV-5	Trust in the central server must be limited. The management of the central server must follow clearly defined governance rules and include all necessary measures to ensure its security. The localization of the central server should allow an effective supervision by the competent supervisory authority. 對中央伺服器之信任須有限度。須依據明確規則管理中央伺服器，且須採取一切必要措施確保其安全。中央伺服器之選址，須可讓權責監管機關實施有效監督。

PRIV-6	<p>A Data Protection Impact Assessment must be carried out and should be made public.</p> <p>須辦理個資保護影響評估並公開其結果。</p>
PRIV-7	<p>The application should only reveal to the user whether they have been exposed to the virus, and, if possible without revealing information about other users, the number of times and dates of exposure.</p> <p>應用程式僅得向使用者揭露其是否曾暴露在病毒中；在不揭露其他使用者資訊的前提下，亦可揭露接觸的次數與日期。</p>
PRIV-8	<p>The information conveyed by the application must not allow users to identify users carrying the virus, nor their movements.</p> <p>應用程式傳遞之資訊不得讓使用者得以識別病毒帶原者及其行動。</p>
PRIV-9	<p>The information conveyed by the application must not allow health authorities to identify potentially exposed users without their agreement.</p> <p>應用程式傳遞之資訊，不得讓衛生主管機關於未經使用者同意下識別潛在感染者。</p>
PRIV-10	<p>Requests made by the applications to the central server must not reveal anything about the virus carrier.</p> <p>應用程式向中央伺服器發出之請求不得揭露病毒帶原者的任何資訊。</p>
PRIV-11	<p>Requests made by the applications to the central server must not reveal any unnecessary information about the user, except, possibly, and only when necessary, for their pseudonymous identifiers and their contact list.</p> <p>應用程式向中央伺服器發出之請求不得揭露使用者的任何非必要資訊；僅得在必要時揭露使用者的假名識別碼與接觸史</p>

	清單。
PRIV-12	Linkage attacks must not be possible. 須避免連結攻擊。
PRIV-13	Users must be able to exercise their rights via the application. 使用者須能夠透過應用程式行使其權利。
PRIV-14	Deletion of the application must result in the deletion of all locally collected data. 刪除應用程式時，須使本地蒐集之全部資料一併刪除。
PRIV-15	The application should only collect data transmitted by instances of the application or interoperable equivalent applications. No data relating to other applications and/or proximity communication devices shall be collected. 應用程式僅得蒐集同類或互通之其他應用程式傳輸之資料，不得蒐集其他應用程式和（或）鄰近通訊裝置之資料。
PRIV-16	In order to avoid re-identification by the central server, proxy servers should be implemented. The purpose of these <i>non-colluding servers</i> is to mix the identifiers of several users (both those of virus carriers and those sent by requesters) before sharing them with the central server, so as to prevent the central server from knowing the identifiers (such as IP addresses) of users. 為避免中央伺服器之再識別行為，應使用代理伺服器。使用此等非串聯伺服器（ <i>non-colluding servers</i> ）之目的是混合數個使用者的識別碼（包括病毒帶原者的識別碼和請求者發出的識別碼），再將其發送給中央伺服器，以防止中央伺服器獲知使用者的識別資訊（如IP位址）。
PRIV-17	The application and the server must be carefully developed and configured in order not to collect any unnecessary data (e.g., no

	<p>identifiers should be included in the server logs, etc.) and in order to avoid the use of any third party SDK collecting data for other purposes.</p> <p>須審慎設計和配置應用程式和伺服器，以避免蒐集任何非必要資料（例如，不得將識別資訊記錄在伺服器日誌中等），並避免使用第三方SDK為其他目的蒐集資料。</p>
--	---

Most contact tracing applications currently being discussed follow basically two approaches when a user is declared infected: they can either send to a server the history of proximity contacts they have obtained through scanning, or they can send the list of their own identifiers that were broadcasted. The following principles are declined¹⁹ according to these two approaches. While these approaches are discussed here, that does not mean other approaches are not possible or even preferable, for example approaches that implement some form of E2E encryption or apply other security or privacy enhancing technologies.

當使用者聲稱被感染時，當前討論中的大部分應用程式採用的處理方式可大致分為兩種：向伺服器發送其透過掃描蒐集的密切接觸史，或是發送其自身已推播的識別碼。下列原則係針對這兩種方式設定*。雖然本文件討論了這兩種方式，但並不表示不存在其他、甚至是更優良的方式，如實施某種形式的端到端（E2E）加密，或採用其他安全或隱私強化技術。

9.1 Principles that apply only when the application sends to the server a list of contacts:

僅適用於應用程式向伺服器發送接觸史清單的原則：

CON-1	The central server must collect the contact history of users reported as positive to COVID-19 as a result of voluntary action
-------	---

* 譯註：此處「declined」疑為原文誤植，似乎應為designed；因此如依原文翻譯為「依據這兩種方式，以下原則不適用」。

	<p>on their part.</p> <p>中央伺服器所蒐集之接觸史記錄，以自願通報新冠肺炎陽性之使用者為限。</p>
CON-2	<p>The central server must not maintain nor circulate a list of the pseudonymous identifiers of users carrying the virus.</p> <p>中央伺服器不得保存或傳播病毒帶原者的假名識別碼清單。</p>
CON-3	<p>Contact history stored on the central server must be deleted once users are notified of their proximity with a positively diagnosed person.</p> <p>向使用者通知其曾與確診者密切接觸後，儲存於中央伺服器的接觸史記錄應立即刪除。</p>
CON-4	<p>Except when the user detected as positive shares his contact history with the central server or when the user makes a request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.</p> <p>除檢測為陽性之使用者與中央伺服器分享其接觸史，或使用使用者請求伺服器確認其是否曾接觸病毒之情形外，使用者的裝置不得發出資料。</p>
CON-5	<p>Any identifier included in the local history must be deleted after X days from its collection (the X value being defined by the health authorities).</p> <p>本地紀錄中儲存的識別碼，應自蒐集日起X日後刪除（X之數值由衛生主管機關定義）。</p>
CON-6	<p>Contact histories submitted by distinct users should not further be processed e.g. cross-correlated to build global proximity maps.</p> <p>個別使用者提交之接觸史資料不得再進階運用，如透過交叉比對構建全球密切接觸分佈圖。</p>

CON-7	<p>Data in server logs must be minimised and must comply with data protection requirements</p> <p>伺服器日誌中的資料須保持最小化，且須符合資料保護要求。</p>
-------	---

9.2 Principles that apply only when the application sends to a server a list of its own identifiers:

僅適用於應用程式向伺服器發送自身識別碼清單的原則：

ID-1	<p>The central server must collect the identifiers broadcast by the application of users reported as positive to COVID-19, as a result of voluntary action on their part.</p> <p>中央伺服器所蒐集之應用程式推播識別碼，以自願通報為新冠肺炎陽性之使用者為限。</p>
ID-2	<p>The central server must not maintain nor circulate the contact history of users carrying the virus.</p> <p>中央伺服器不得保存或傳播病毒帶原者的接觸史記錄。</p>
ID-3	<p>Identifiers stored on the central server must be deleted once they were distributed to the other applications.</p> <p>向其他應用程式推播後，儲存於中央伺服器的識別碼應立即刪除。</p>
ID-4	<p>Except when the user detected as positive shares his identifiers with the central server, no data must leave the user's equipment or when the user makes a request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.</p> <p>除檢測為陽性之使用者與中央伺服器分享其識別碼，或使用者請求伺服器確認其是否曾接觸病毒之情形外，使用者的裝置不得發出資料。</p>

ID-5	Data in server logs must be minimised and must comply with data protection requirements 伺服器日誌中的資料須保持最小化，且須符合資料保護要求。
------	--

Guidelines



Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak

關於在新冠肺炎（COVID-19）防疫期間為科學研究目的運用健康資料之指引03/2020

Adopted on 21 April 2020

2020年4月21日通過

Table of contents

目錄

1. Introduction 導言	4
2. Application of the GDPR GDPR之適用	4
3. Definitions 定義	6
3.1 “Data concerning health” 「健康資料」	6
3.2 “Processing for the purpose of scientific research” 「為科學研究目的運用資料」	7
3.3 “Further processing” 「進階運用」	8
4. Legal basis for the processing 運用之法律依據	10
4.1 Consent 同意	10
4.2 National legislations 國家立法	13
5. Data protection principles 資料保護原則	14
5.1 Transparency and information to data subjects 透明化與對當事人提供資訊	15
5.1.1 When must the data subject be informed? 何時須告知當事人?	16
5.1.2 Exemptions 例外	17
5.2 Purpose limitation and presumption of compatibility 目的限制與推定相容	20
5.3 Data minimisation and storage limitation 資料最小化和儲存限制	22
5.4 Integrity and confidentiality 完整性和機密性	23
6. Exercise of the rights of data subjects 當事人權利之行使	24
7. International data transfers for scientific research purposes 為科學研究目的實施之國際資料傳輸	25
8. Summary 結論	31

The European Data Protection Board

Having regard to Article 70 (1) (e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

歐盟個人資料保護委員會

依據歐洲議會與歐盟理事會於2016年4月27日通過之「關於運用*個人資料時對自然人之保護與確保此等資料之自由流通，以及廢除指令95/46/EC的歐盟規則2016/679/EU」（下稱GDPR）第70條第1項第e款；

依據歐洲經濟區聯合委員會於2018年7月6日第154/2018號決定修改之歐洲經濟區（EEA）協議，尤其是附件11及其議定書37；

依據「歐盟個人資料保護委員會議事規則」第12條和第22條；

通過以下指引：

* 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」。

1. INTRODUCTION

導言

1. Due to the COVID-19 pandemic, there are currently great scientific research efforts in the fight against the SARS-CoV-2 in order to produce research results as fast as possible.

由於新冠肺炎（COVID-19）疫情蔓延，許多對抗新型冠狀病毒（SARS-CoV-2）科學研究正在進行之中，以求盡快產出研究結果。

2. At the same time, legal questions concerning the use of health data pursuant to Article 4 (15) GDPR for such research purposes keep arising. The present guidelines aim to shed light on the most urgent of these questions such as the legal basis, the implementation of adequate safeguards for such processing of health data and the exercise of the data subject rights.

於此同時，關於GDPR第4條第15款所規範的健康資料之運用，許多法律問題不斷產生。本指引旨在釐清其中最具緊迫性的問題，如法律依據、運用此等健康資料時採行之適當安全維護措施，以及當事人權利之行使等。

3. Please note that the development of a further and more detailed guidance for the processing of health data for the purpose of scientific research is part of the annual work plan of the EDPB. Also, please note that the current guidelines do not revolve around the processing of personal data for epidemiological surveillance.

請注意，為科學研究目的運用健康資料議題，制定一個進一步的、更為詳盡的指導，乃歐盟個人資料保護委員會（EDPB）年度工作計畫之一部分。此外，請注意本指引並未涉及為流行病學監測目的運用個人資料。

2. APPLICATION OF THE GDPR

GDPR之適用

4. Data protection rules (such as the GDPR) do not hinder measures taken in the fight against the COVID- 19 pandemic.¹ The GDPR is a broad piece of

legislation and provides for several provisions that allow to handle the processing of personal data for the purpose of scientific research connected to the COVID-19 pandemic in compliance with the fundamental rights to privacy and personal data protection.² The GDPR also foresees a specific derogation to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for these purposes of scientific research.³

資料保護規範（如GDPR）並不妨礙實施疫情防控措施¹。GDPR係一部廣泛法律，其部分規定皆容許在遵循隱私之基本權利與個人資料保護下，為新冠肺炎防疫相關之科學研究目的運用個人資料²。GDPR亦預見，為科學研究目的³之必要，對部分特種個資(如健康資料)運用之禁止會有具體的例外。

5. Fundamental Rights of the EU must be applied when processing health data for the purpose of scientific research connected to the COVID-19 pandemic. Neither the Data Protection Rules nor the Freedom of Science pursuant to Article 13 of the Charter of Fundamental Rights of the EU have precedence over the other. Rather, these rights and freedoms must be carefully assessed and balanced, resulting in an outcome which respects the essence of both.

為新冠肺炎防疫相關之科學研究目的運用健康資料時，須保障歐盟承認之基本權利。資料保護規範和歐盟「基本權利憲章」第13條規定的科學自由間，並無何者優先之關係。而是須審慎評估和平衡這些權利與自由，以求兩者之本質皆獲得尊重之結果。

¹ See the Statement of the EDPB from 19.3.2020 on the general processing of personal data in the context of the COVID-19 outbreak, available at https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en.

見EDPB「關於新冠肺炎防疫期間一般性運用個人資料之聲明」（2020年3月19日版），請參閱：https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en。

² See for example Article 5 (1) (b) and (e), Article 14 (5) (b) and Article 17 (3) (d) GDPR.
示例見GDPR第5條第1項第b款和第e款，第14條第5項第b款和第17條第3項第d款。

³ See for example Article 9 (2) (j) and Article 89 (2) GDPR.
示例見GDPR第9條第2項第j款和GDPR第89條第2項。

3. DEFINITIONS

定義

6. It is important to understand which processing operations benefit from the special regime foreseen in the GDPR and elaborated on in the present guidelines. Therefore, the terms “data concerning health”, “processing for the purpose of scientific research” as well as “further processing” (also referred to as “primary and secondary usage of health data”) must be defined.

重要的是瞭解哪種運用作業得受益於GDPR預見並在本指引中闡明之特殊制度。因此，須定義「健康資料」、「為科學研究目的運用」與「進階運用」（亦稱健康資料之初級使用（primary usage）和次級使用（secondary usage））。

3.1 “Data concerning health”

「健康資料」

7. According to Article 4 (15) GDPR, “data concerning health” means *“personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”*. As indicated by Recital 53, data concerning health deserves higher protection, as the use of such sensitive data may have significant adverse impacts for data subjects. In the light of this and the relevant jurisprudence of the European Court of Justice (“ECJ”),⁴ the term “data concerning health” must be given a wide interpretation.

依據GDPR第4條第15款，「健康資料」係指「與自然人之身體或精神健康有關之個人資料，包括揭示其健康狀況之健康照護服務之提供」。如前言第53點所述，健康資料需要更高程度之保護，因運用這些敏感資料可能對當事人造成重大不利影響。有鑑於此，並依歐洲法院（ECJ）⁴之相關實務見解，「健康資料」須作廣義解釋。

⁴ See for example, regarding the Directive 95/46/EC ECJ 6.3.2003, C-101/01 (Lindqvist) paragraph 50. 示例見，關於指令95/46/EC，歐洲法院2003年11月6日（譯註：原文3月6日應為誤植）第C-

8. Data concerning health can be derived from different sources, for example:

健康資料可取自多種來源，例如：

1. Information collected by a health care provider in a patient record (such as medical history and results of examinations and treatments).

健康照護提供者自病患檔案中蒐集之資訊（如病史、檢查和治療結果）。

2. Information that becomes health data by cross referencing with other data thus revealing the state of health or health risks (such as the assumption that a person has a higher risk of suffering heart attacks based on the high blood pressure measured over a certain period of time).

透過與其他資料交叉比對，並因此揭示健康狀況或健康風險而構成健康資訊（如基於一定期間內對特定個人測得之偏高血壓數值，推測該人有較高心臟病發作風險）。

3. Information from a “self check” survey, where data subjects answer questions related to their health (such as stating symptoms).

經「自我評估」調查獲知之資訊，該等調查中，由當事人回答與其健康相關問題（如描述症狀）。

4. Information that becomes health data because of its usage in a specific context (such as information regarding a recent trip to or presence in a region affected with COVID-19 processed by a medical professional to make a diagnosis).

因特定情形下使用而成為健康資料之資訊（如醫療人員為作出診斷而運用「最近曾前往新冠肺炎疫區」或位於疫區之資訊）。

3.2 “Processing for the purpose of scientific research”

「為科學研究目的運用資料」

9. Article 4 GDPR does not entail an explicit definition of “processing for the

101/01號案件（Lindqvist）判決，第50段。

purpose of scientific research”. As indicated by Recital 159, “the term *processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union’s objective under Article 179 (1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health.*”

GDPR第4條並未明確定義「為科學研究目的運用資料」。如前言第159點所述，「『為科學研究目的運用資料』此一術語應做廣義解釋，包括技術開發和演示、基礎研究、應用研究和私人資助之研究等。此外，應考量歐盟運作條約（TFEU）第179條第1項規定之構建歐洲研究區之歐盟目標。科學研究目的還應包括公共衛生領域符合公共利益之研究。」

10. The former Article 29-Working-Party has already pointed out that the term may not be stretched beyond its common meaning though and understands that “scientific research” in this context means “a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice”.⁵

雖前第29條工作小組已指出，該術語之擴張解釋尚不得超出其通常含義；且該小組認為，此時「科學研究」係指「依相關行業方法與道德標準建構，且符合最佳實務的研究計畫」⁵。

3.3 “Further processing”

「進階運用」

11. Finally, when talking about “processing of health data for the purpose of scientific research”, there are two types of data usages:

⁵ See the Guidelines on Consent under Regulation 2016/679 of the former Article 29 Working-Party from 6.7.2018, WP259 rev.01, 17EN, page 27 (endorsed by the EDPB). Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

見前第29條工作小組「關於第2016/679號規則(GDPR)中的同意之指引」（2018年7月6日版），WP259 rev.01，17EN，頁27（EDPB採認），請參閱：https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051。

最後，關於「為科學研究目的運用健康資料」，有兩種使用方式：

1. Research on personal (health) data which consists in the use of data directly collected for the purpose of scientific studies (“primary use”).

為科學研究目的直接蒐集的資料，對個人（健康）資料進行研究（「初級使用」）之使用。

2. Research on personal (health) data which consists of the further processing of data initially collected for another purpose (“secondary use”).

為其他目的而蒐集的資料，對個人（健康）資料進行研究（「次級使用」）之進階運用。

12. **Example 1:** For conducting a clinical trial on individuals suspected to be infected with COVID-19, health data are collected and questionnaires are used. This is a case of “primary use” of health data as defined above.

示例1：為對疑似感染新冠肺炎的個體進行臨床試驗，蒐集其健康資料並使用問卷調查。此即前開定義的健康資料之「初級使用」。

13. **Example 2:** A data subject has consulted a health care provider as a patient regarding symptoms of the SARS-CoV-2. If health data recorded by the health care provider is being used for scientific research purposes later on, this usage is classified as further processing of health data (secondary use) that has been collected for another initial purpose.

示例2：當事人曾以病患身分就新冠肺炎症狀向健康照護者進行諮詢。若該健康照護者記錄之健康資料後來被用於科學研究目的，此種使用會被歸類為其他初始目的蒐集之健康資料的進階運用（次級使用）。

14. The distinction between scientific research based on primary or secondary usage of health data will become particularly important when talking about the legal basis for the processing, the information obligations and the purpose limitation principle pursuant to Article 5 (1) (b) GDPR as outlined below.

當涉及運用資料之法律依據、資訊提供義務（information obligation）

以及GDPR第5條第1項第b款規定之目的限制原則時，區分科學研究中健康資料的初級使用和次級使用尤為重要，詳述如下。

4. LEGAL BASIS FOR THE PROCESSING

運用之法律依據

15. All processing of personal data concerning health must comply with the principles relating to processing set out in Article 5 GDPR and with one of the legal grounds and the specific derogations listed respectively in Article 6 and Article 9 GDPR for the lawful processing of this special category of personal data.⁶

對健康資料之一切運用皆須遵守GDPR第5條規定的運用之各項原則；還須具備GDPR第6條規定的合法要件之一，與第9條規定的合法運用特種個資之明確例外之一⁶。

16. Legal bases and applicable derogations for processing health data for the purpose of scientific research are provided for respectively in Article 6 and Article 9. In the following section, the rules concerning consent and respective national legislation are addressed. It has to be noted that there is no ranking between the legal bases stipulated in the GDPR.

第6條和第9條分別規定了為科學研究目的運用健康資料的法律依據及可適用之例外。本節將討論同意以及個別國家立法的相關規範。應注意，GDPR規定之各項法律依據間並無位階差別。

4.1 Consent

同意

17. The consent of the data subject, collected pursuant to Article 6 (1) (a) and Article 9 (2) (a) GDPR, may provide a legal basis for the processing of data concerning health in the COVID-19 context.

依GDPR第6條第1項第a款和第9條第2項第a款獲得之當事人同意，可

⁶ See for example, regarding the Directive 95/46/EC ECJ 13.5.2014, C-131/12 (Google Spain), paragraph 71.

示例見，關於指令95/46/EC，歐洲法院2014年5月13日第C-131/12號案件（Google Spain）判決，第71段。

作為在新冠肺炎防疫期間運用健康資料之法律依據。

18. However, it has to be noted that all the conditions for explicit consent, particularly those found in Article 4 (11), Article 6 (1) (a), Article 7 and Article 9 (2) (a) GDPR, must be fulfilled. Notably, consent must be freely given, specific, informed, and unambiguous, and it must be made by way of a statement or “clear affirmative action”.

然而，應注意須符合明確同意之各項要件，特別是GDPR第4條第11款、第6條第1項第a款、第7條和第9條第2項第a款規定之要件。尤其是，同意應自主給予、特定、知情且非模糊，且須以聲明或「清楚肯定行為」為之。

19. As stated in Recital 43, consent cannot be considered freely given if there is a clear imbalance between the data subject and the controller. It is therefore important that a data subject is not pressured and does not suffer from disadvantages if they decide not to give consent. The EDPB has already addressed consent in the context of clinical trials.⁷ Further guidance, particularly on the topic of explicit consent, can be found in the consent guidelines of the former Article 29-Working-Party.⁸

如前言第43點所言，若當事人與控管者間存在明顯不對等，則不得認為同意係自主給予。因此，有必要確保當事人未被強迫，且不因拒絕同意而承受不利益。EDPB已就臨床試驗所涉之同意發表意見⁷。另可自前第29條工作小組之同意指引獲得進一步指導，特別是關於明確同意⁸。

20. **Example:** A survey is conducted as part of a non-interventional study on

⁷ See Opinion 3/2019 of the EDPB from 23.1.2019 on concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), available at https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en.

見EDPB「關於臨床試驗規則（CTR）和一般資料保護規則（GDPR）間互動問答集之意見3/2019」（2019年1月23日版），請參閱：https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en。

⁸ Guidelines on Consent under Regulation 2016/679 of the former Article 29 Working-Party from 6.7.2018, WP259 rev.01, 17EN, page 18 (endorsed by the EDPB).

前第29條工作小組「關於第2016/679號規則(GDPR)中的同意之指引」（2018年7月6日版），WP259 rev.01, 17EN，頁18（EDPB採認）。

a given population, researching symptoms and the progress of a disease. For the processing of such health data, the researchers may seek the consent of the data subject under the conditions as stipulated in Article 7 GDPR.

示例：作為非介入性（non-interventional）研究之一部分，對特定群體進行調查，研究某一疾病之症狀與發展。為運用此等健康資料，研究人員得依GDPR第7條所明定之要件徵求當事人同意。

21. In the view of the EDPB, the example above is *not* considered a case of “clear imbalance of power” as mentioned in Recital 43 and the data subject should be able to give the consent to the researchers.⁹ In the example, the data subjects are not in a situation of whatsoever dependency with the researchers that could inappropriately influence the exercise of their free will and it is also clear that it will have no adverse consequences if they refuse to give their consent.

EDPB認為，上開示例中並不存在前言第43點所述之「權力明顯不平等」，且當事人應可對研究人員給予同意⁹。該示例中，當事人與研究人員並無任何依賴關係，以致影響其表達自由意志，而且，當事人並不會因拒絕同意而承受不利後果。

22. However, researchers should be aware that if consent is used as the lawful basis for processing, there must be a possibility for individuals to withdraw that consent at any time pursuant to Article 7 (3) GDPR. If consent is withdrawn, all data processing operations that were based on consent remain lawful in accordance with the GDPR, but the controller shall stop the processing actions concerned and if there is no other lawful basis justifying the retention for further processing, the data should be deleted by the controller.¹⁰

然而，研究人員應注意，若以同意作為運用之合法依據，依GDPR第7條第3項，相關個人須能夠隨時撤回同意。撤回同意後，依GDPR，此

⁹ Assuming that the data subject has not been pressured or threatened with disadvantages when not giving his or her consent.

假設當事人未被強迫，且不受拒絕同意時之不利益威脅。

前基於同意實施之一切資料運用作業仍為合法，但控管者須停止相關運用行為，且若無可正當保留資料作進階運用的其他合法依據，控管者應刪除該資料¹⁰。

4.2 National legislations

國家立法

23. Article 6 (1) e or 6 (1) f GDPR in combination with the enacted derogations under Article 9 (2) (j) or Article 9 (2) (i) GDPR can provide a legal basis for the processing of personal (health) data for scientific research. In the context of clinical trial this has already been clarified by the Board.¹¹

GDPR第6條第1項第e款或第f款，結合第9條第2項第j款或第i款之例外規定，能夠作為為科學研究目的運用個人（健康）資料的法律依據。在臨床試驗領域，委員會對此已做說明¹¹。

24. **Example:** A large population based study conducted on medical charts of COVID-19 patients.

示例：以新冠肺炎患者之病歷，進行大規模族群（population based）研究。

25. As outlined above, the EU as well as the national legislator of each Member State may enact specific laws pursuant to Article 9 (2) (j) or Article 9 (2) (i) GDPR to provide a legal basis for the processing of health data for the purpose of scientific research. Therefore, the conditions and the extent for such processing *vary* depending on the enacted laws of the particular Member State.

如前所述，歐盟以及各會員國之立法者得依GDPR第9條第2項第j款或第i款制定具體法律，作為為科學研究目的運用健康資料的法律依據。因此，此等運用之條件與程度依具體會員國所制定之法律而有所不同。

¹⁰ See Article 17 (1) (b) and (3) GDPR.
見GDPR第17條第1項第b款和第3項。

¹¹ See Opinion 3/2019 of the EDPB from 23.1.2019, page 7.
見EDPB「意見3/2019」（2019年1月23日版），頁7。

26. As stipulated in Article 9 (2) (i) GDPR, such laws shall provide “*for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy*”. As similarly stipulated in Article 9 (2) (j) GDPR, such enacted laws “*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 the interests of the data subject*”.

GDPR第9條第2項第i款規定，此等法律須規定「保障當事人權利與自由的適當具體措施，特別是職業秘密」。GDPR第9條第2項第j款也有類似規定，即此等法律「須與其追求之目的間合乎比例，尊重資料保護權利之本質，且規定保障當事人基本權利和利益之適當具體措施」。

27. Furthermore, such enacted laws must be interpreted in the light of the principles pursuant to Article 5 GDPR and in consideration of the jurisprudence of the ECJ. In particular, derogations and limitations in relation to the protection of data provided in Article 9 (2) (j) and Article 89 GDPR must apply only in so far as is strictly necessary.¹²

此外，解釋此等法律時，須以GDPR第5條之各項原則為依據，並考量歐洲法院的實務見解。特別是，GDPR第9條第2項第j款和第89條關於資料保護之例外與限制規定，須在絕對必要之情況下始有其適用¹²。

5. DATA PROTECTION PRINCIPLES

資料保護原則

28. The principles relating to processing of personal data pursuant to Article 5 GDPR shall be respected by the controller and processor, especially considering that a great amount of personal data may be processed for the purpose of scientific research. Considering the context of the present guidelines, the most important aspects of these principles are addressed in the following.

¹² See for example, regarding the Directive 95/46/EC ECJ 14.2.2019, C-345/17 (Buivids) paragraph 64. 示例見，關於指令95/46/EC，歐洲法院2019年2月14日第C-345/17號案件（Buivids）判決，第64段。

特別考量到為科學研究之目的，可能運用大量個人資料，因此控管者和受託運用者應遵守GDPR第5條之個人資料運用原則。考量本指引之背景，以下提出這些原則最重要之面向。

5.1 Transparency and information to data subjects

透明化與對當事人提供資訊

29. The principle of transparency means that personal data shall be processed fairly and in a transparent manner in relation to the data subject. This principle is strongly connected with the information obligations pursuant to Article 13 or Article 14 GDPR.

透明化原則係指，個人資料之運用應公平合理並對當事人以透明之方式為之。該原則與GDPR第13條和第14條規定之資訊提供義務密切相關。

30. In general, a data subject must be individually informed of the existence of the processing operation and that personal (health) data is being processed for scientific purposes. The information delivered should contain all the elements stated in Article 13 or Article 14 GDPR.

一般而言，應個別告知當事人資料運用作業之存在，以及個人（健康）資料係為科學目的運用。所提供之資訊應包含GDPR第13條和第14條規定之各項要素。

31. It has to be noted that researchers often process health data that they have not obtained directly from the data subject, for instance using data from patient records or data from patients in other countries. Therefore, Article 14 GDPR, which covers information obligations where personal data is not collected directly from the data subject, will be the focus of this section.

應注意，研究人員所運用之個人資料，往往並非直接取自當事人，如取自病患紀錄之資料，或其他國家病患之資料。因此，GDPR第14條規定之非直接向當事人蒐集資料時的資訊(提供)義務，乃本節焦點。

5.1.1 When must the data subject be informed?

何時須告知當事人？

32. When personal data have not been obtained from the data subject, Article 14 (3) (a) GDPR stipulates that the controller shall provide the information *“within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed”*.

對於非直接取自當事人的個人資料，GDPR第14條第3項第a款規定，控管者須「考量個人資料運用之具體情形，在取得該個人資料後的合理期間內，至遲於一個月內」，提供相關資訊。

33. In the current context, it has to be particularly noted that according to Article 14 (4) GDPR, where *“the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose”*.

於目前情況下，尤應注意，依據GDPR第14條第4項規定，當「控管者想在個人資料之蒐集目的外，進階運用個人資料，則應在該進階運用前，向當事人提供該其他目的之相關資訊」。

34. In the case of the further processing of data for scientific purposes and taking into account the sensitivity of the data processed, an appropriate safeguard according to Article 89 (1) is to deliver the information to the data subject within a reasonable period of time *before* the implementation of the new research project. This allows the data subject to become aware of the research project and enables the possibility to exercise his/her rights beforehand.

為科學研究目的進階運用資料時，考量所運用資料之敏感性，第89條第1項規定之適當安全維護措施之一，係在執行新的研究計畫前之適當期間內，提供當事人相關資訊。這使當事人得以獲知研究計畫，並使其具有在事前行使其權利之可能性。

5.1.2 Exemptions

例外

35. However, Article (14) (5) GDPR stipulates four exemptions of the information obligation. In the current context, the exemption pursuant to Article (14) (5) (b) (“proves impossible or would involve a disproportionate effort”) and (c) (“obtaining or disclosure is expressly laid down by Union or Member State law”) GDPR are of particular relevance, especially for the information obligation pursuant to Article 14 (4) GDPR.

然而，GDPR第14條第5項規定了資訊提供義務的四項例外。於目前情況下，尤其是就GDPR第14條第4項規定的資訊提供義務而言，最具關連性者為GDPR第14條第5項第b款（「證明為不可能或將涉及不成比例之付出」）和第c款（「歐盟法或會員國法明文規定之取得或揭露」）的例外。

5.1.2.1 Proves impossible

證明為不可能

36. In its Guidelines regarding the principle of Transparency,¹³ the former Article 29-Working-Party has already pointed out that *“the situation where it “proves impossible” under Article 14 (5) (b) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus, if a data controller seeks to rely on this exemption it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the “impossibility” no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects.”*

在透明化原則之相關指引中¹³，前第29條工作小組已指出，「第14條第5項第b款中所謂當提供資訊被『證明為不可能』之情形，應屬一種或可提供全部資訊、或完全無法提供之情形，因為『不可能』並沒有程度上的區分。因此，若資料控管者試圖援用此項例外，則必須證明有實際上阻止其向當事人提供有關資訊之因素。若在一段期間後，導致『不可能性』之因素已不存在，且可向當事人提供資訊時，資料控管者應立即為之。實際上，僅在少數情況下資料控管者可證明其事實上不可能向當事人提供資訊。」

5.1.2.2 Disproportionate effort

不成比例之付出

37. In determining what constitutes disproportionate effort, Recital 62 refers to the number of data subjects, the age of the data and appropriate safeguards in place as possible indicative factors. In the Transparency Guidelines mentioned above,¹⁴ it is recommended that the controller should therefore carry out a balancing exercise to assess the effort involved to provide the information to data subjects against the impact and effects on the data subject if they are not provided with the information.

於決定如何構成不成比例之付出時，前言第62點提到，當事人之數量、資料之年代和採行之適當安全維護措施是可能的指示性因素。前開透明化指引¹⁴建議，控管者應進行衡量比較，評估提供資訊予當事人之工作量，以及若未提供該資訊予當事人將對其產生之影響和結果。

¹³ See the Guidelines on transparency under Regulation 2016/679 of the former Article-29 Working-Party from 11.4.2018, WP260 rev.01, 17/EN, page 29 (endorsed by the EDPB). Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

見前第29條工作小組「第2016/679號規則 (GDPR)的透明化指引」(2018年4月11日版)，WP260 rev.01, 17/EN，頁29 (EDPB採認)，請參閱：https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227。

¹⁴ Guidelines on transparency under Regulation 2016/679 of the former Article-29 Working-Party from 11.4.2018, WP260 rev.01, 17/EN, page 31 (endorsed by the EDPB).

前第29條工作小組「第2016/679號規則 (GDPR)的透明化指引」(2018年4月11日版)，WP260 rev.01, 17/EN，頁31 (EDPB採認)。

38. **Example:** A large number of data subjects where there is no available contact information could be considered as a disproportionate effort to provide the information.

示例：若當事人數量大且無可用之聯絡資訊，可認為提供資訊將構成不成比例之付出。

5.1.2.3 *Serious impairment of objectives*

對目的之嚴重損害

39. To rely on this exception, data controllers must demonstrate that the provision of the information set out in Article 14 (1) *per se* would render impossible or seriously impair the achievement of the objectives of the processing.

為援用此項例外，資料控管者必須證明提供第14條第1項規定之資訊本身將使運用資料之目的無法達成或嚴重受損。

40. In a case where the exemption of Article (14) (5) (b) GDPR applies, “the controller shall take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available”.

若適用GDPR第14條第5項第b款規定之例外，則「控管者應採取適當措施保護當事人之權利和自由以及正當利益，包括公開該等資訊。」

5.1.2.4 *Obtaining or disclosure is expressly laid down by Union or Member State law*

歐盟法或會員國法明文規定之取得或揭露

41. Article 14 (5) (c) GDPR allows for a derogation of the information requirements in Articles 14 (1), (2) and (4) insofar as the obtaining or disclosure of personal data “is expressly laid down by Union or Member State law to which the controller is subject”. This exemption is conditional upon the law in question providing “appropriate measures to protect the data subject’s legitimate interests”. As stated in the above mentioned Transparency Guidelines,¹⁵ such law must directly address the data controller and the obtaining or disclosure in question should be

mandatory upon the data. When relying on this exemption, the EDPB recalls that the data controller must be able to demonstrate how the law in question applies to them and requires them to either obtain or disclose the personal data in question.

依GDPR第14條第5項第c款，若取得或揭露個人資料係「依據控管者適用之歐盟法或會員國法律明文規定」，則可免除第14條第1項、第2項和第4項規定之提供資訊要求。此一例外之條件是，相關法律提供「保護當事人正當利益之適當措施」。如前開透明化指引¹⁵所述，此等法律須直接規範資料控管者，且取得或揭露資料應具強制性。援用此一例外時，EDPB重申，資料控管者必須能夠證明其適用該相關法律，且該法律要求其取得或揭露相關個人資料。

5.2 Purpose limitation and presumption of compatibility

目的限制與相容性推定

42. As a general rule, data shall be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes” pursuant to Article 5 (1) (b) GDPR.

一般而言，依據GDPR第5條第1項b款，資料之「蒐集須有特定、明確且正當之目的，且不得以該等目的不相容之方式為進階運用」。

43. However the “compatibility presumption” provided by Article 5 (1) (b) GDPR states that “further processing for [...] scientific research purposes [...] shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes”. This topic, due to its horizontal and complex nature, will be considered in more detail in the planned EDPB guidelines on the processing of health data for the purpose of scientific research.

然而，GDPR第5條第1項第b款之「相容性推定」規定，「依第89條第1項，為……科學研究目的……之進階運用，不得被視為與初始目的

¹⁵ Guidelines on transparency under Regulation 2016/679 of the former Article-29 Working-Party from 11.4.2018, WP260 rev.01, 17/EN, page 32 (endorsed by the EDPB).

見前第29條工作小組「關於第2016/679號規則 (GDPR)中的透明化之指引」（2018年4月11日版），WP260 rev.01, 17/EN，頁32（EDPB採認）。

不相容」。此一議題，由於其水平性（horizontal）和複雜性，將在EDPB計劃發布之關於為科學研究目的運用健康資料的指引中，提供更深入之探討。

44. Article 89 (1) GDPR stipulates that the processing of data for research purposes *“shall be subject to appropriate safeguards”* and that those *“safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner”*.

GDPR第89條第1項規定，為研究目的運用資料，「應有適當安全維護措施」，且此等「安全維護措施應確保採行技術性和組織性措施，特別是為確保遵守資料最小化原則。在能滿足其目的之前提下，此等措施可能包括假名化處理」。

45. The requirements of Article 89 (1) GDPR emphasise the importance of the data minimisation principle and the principle of integrity and confidentiality as well as the principle of data protection by design and by default (see below).¹⁶ Consequently, considering the sensitive nature of health data and the risks when re-using health data for the purpose of scientific research, strong measures must be taken in order to ensure an appropriate level of security as required by Article 32 (1) GDPR. GDPR第89條第1項之要件強調資料最小化原則、完整性和機密性原則、以及資料保護設計（by design）和預設（by default）原則（見下文）¹⁶。因此，考量健康資料的敏感本質，以及為科學研究目的再使用健康資料之風險，須採取有力措施，確保實現GDPR第32條第1項規定的適當安全程度。

¹⁶ Also see the Guidelines 4/2019 of the EDPB from 13.11.2019 on Data Protection by Design and by Default (version for public consultation), available at https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

另見，EDPB「關於資料保護設計和預設之指引4/2019」（2019年11月13日，公告徵求意見版），請參閱：https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en。

5.3 Data minimisation and storage limitation

資料最小化和儲存限制

46. In scientific research, data minimisation can be achieved through the requirement of specifying the research questions and assessing the type and amount of data necessary to properly answer these research questions. Which data is needed depends on the purpose of the research even when the research has an explorative nature and should always comply with the purpose limitation principle pursuant to Article 5 (1) (b) GDPR. It has to be noted that the data has to be anonymised where it is possible to perform the scientific research with anonymised data.

科學研究中，可透過詳細說明研究問題的要求、評估充分解決研究問題所需之資料類型與數量，實現資料最小化。對資料的需求取決於研究目的（即便是探索式研究也是如此），且應始終遵守GDPR第5條第1項第b款規定的目的限制原則。亦應注意，若可使用匿名資料進行該科學研究，則應將資料匿名化。

47. In addition, proportionate storage periods shall be set. As stipulated by Article 5 (1) (e) GDPR *“personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving [...] scientific purposes [...] in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject”*

此外，應設定合乎比例之儲存期間。根據GDPR第5條第1項第e款規定，「專為歸檔……科學目的……運用個人資料，依第89條第1項執行本規則規定之適當技術性和組織性措施以保障當事人之權利與自由者，個人資料得儲存較長時間」。

48. In order to define storage periods (timelines), criteria such as the length and the purpose of the research should be taken into account. It has to be noted that national provisions may stipulate rules concerning the storage period as well.

為確定儲存期間（時限），應考慮研究之時間長短和目的等標準。應注意，國家法律亦可能就儲存期間明訂相關規定。

5.4 Integrity and confidentiality

完整性和機密性

49. As mentioned above, sensitive data such as health data merit higher protection as their processing is likelier to lead to negative impacts for data subjects. This consideration especially applies in the COVID-19 outbreak as the foreseeable re-use of health data for scientific purposes leads to an increase in the number and type of entities processing such data.

如前所述，由於健康資料等敏感資料之運用更易導致對當事人之不利影響，此等資料需要更高程度之保護。新冠肺炎防疫期間，這一考量尤其重要，因為可以預見為科學目的對健康資料進行再使用，將導致運用此等資料之實體的數量與類型大幅增加。

50. It has to be noted that the principle of integrity and confidentiality must be read in conjunction with the requirements of Article 32 (1) GDPR and Article 89 (1) GDPR. The cited provisions must be fully complied with. Therefore, considering the high risks as outlined above, appropriate technical and organisational up-to-date measures must be implemented to ensure a sufficient level of security.

還應注意，對完整性和機密性原則之理解，須結合GDPR第32條第1項和GDPR第89條第1項。且須完全遵守此兩條文。因此，考量到前述之高度風險，必須實施適當且先進的技術性和組織性措施，以確保足夠的安全程度。

51. Such measures should *at least* consist of pseudonymisation,¹⁷ encryption, non-disclosure agreements and strict access role distribution, restrictions as well as logs. It has to be noted that national provisions may stipulate concrete technical requirements or other safeguards such as adherence to professional secrecy rules.

此等措施至少應包括假名化¹⁷、加密、保密協議和嚴格存取權限分配、限制措施和日誌（log）。應注意，國家法律亦可能規定具體技術要求或其他安全維護措施，如遵守職業保密規範等。

52. Furthermore, a data protection impact assessment pursuant to Article 35 GDPR must be carried out when such processing is *“likely to result in a high risk to the rights and freedoms of natural persons”* pursuant to Article 35 (1) GDPR. The lists pursuant to Article 35 (4) and (5) GDPR shall be taken into account.

此外，依據GDPR第35條第1項規定，若運用「可能對自然人之權利和自由造成高風險」，則應辦理GDPR第35條規定的個資保護影響評估。應考慮GDPR第35條第4項和第5項規定的運用類型清單。

53. At this point, the EDPB emphasises the importance of data protection officers. Where applicable, data protection officers should be consulted on processing of health data for the purpose of scientific research in the context of the COVID-19 outbreak.

於此，EDPB強調個資保護長之重要性。在可行情況下，新冠肺炎防疫期間，為科學研究目的運用健康資料時，應諮詢個資保護長。

54. Finally, the adopted measures to protect data (including during transfers) should be properly documented in the record of processing activities.

最後，所採取之資料保護措施（包括資料傳輸期間的措施），應在運用活動檔案中予以適當記錄。

6. EXERCISE OF THE RIGHTS OF DATA SUBJECTS

當事人權利之行使

55. In principle, situations as the current COVID-19 outbreak do not suspend or restrict the possibility of data subjects to exercise their rights pursuant to Article 12 to 22 GDPR. However, Article 89 (2) GDPR allows the

¹⁷ It has to be noted that personal (health data) that has been pseudonymised is still regarded as “personal data” pursuant to Article 4 (1) GDPR and must not be confused with “anonymised data” where it is no longer possible for anyone to refer back to individual data subjects. See for example Recital 28.

應注意，經假名化之個人資料（健康資料）仍為GDPR第4條第1款定義之「個人資料」，且不應與「匿名資料」（任何人皆無法回復識別個別當事人）混淆。示例見前言第28點。

national legislator to restrict (some) of the data subject's rights as set in Chapter 3 of the regulation. Because of this, the restrictions of the rights of data subjects *may vary* depending on the enacted laws of the particular Member State.

原則上，當前新冠肺炎疫情等狀況不會中止或限制當事人依GDPR第12條至第22條行使權利。然而，GDPR第89條第2項允許國家立法者限制當事人依GDPR第三章享有的（某些）權利。因此，對當事人權利的限制，可能因具體會員國所制定之法律而有所不同。

56. Furthermore, some restrictions of the rights of data subjects can be based directly on the Regulation, such as the access right restriction pursuant to Article 15 (4) GDPR and the restriction of the right to erasure pursuant to Article 17 (3) (d) GDPR. The information obligation exemptions pursuant to Article 14 (5) GDPR have already been addressed above.

此外，可直接基於GDPR對當事人的權利課予某些限制，如依GDPR第15條第4項限制近用權，以及依GDPR第17條第3項第d款限制刪除權。GDPR第14條第5項規定之資訊提供義務之例外已於上文討論。

57. It has to be noted that, in the light of the jurisprudence of the ECJ, all restrictions of the rights of data subjects must apply only in so far as it is strictly necessary.¹⁸

應注意，歐洲法院的實務見解認為，對當事人權利的任何限制，皆應限於必要範圍內¹⁸。

7. INTERNATIONAL DATA TRANSFERS FOR SCIENTIFIC RESEARCH PURPOSES

為科學研究目的實施之國際資料傳輸

58. Within the context of research and specifically in the context of the COVID-19 pandemic, there will probably be a need for international cooperation that may also imply international transfers of health data for

¹⁸ See for example, regarding the Directive 95/46/EC ECJ 14.2.2019, C-345/17 (Buivids) paragraph 64. 示例見，歐洲法院2019年2月14日第C-345/17號案件（Buivids）關於95/46/EC指令判決，第64段。

the purpose of scientific research outside of the EEA.

為研究目的，特別是新冠肺炎防疫相關研究，可能需要進行國際合作，亦可能意味著，為於歐洲經濟區外科學研究之目的，進行健康資料國際傳輸。

59. When personal data is transferred to a non-EEA country or international organisation, in addition to complying with the rules set out in GDPR,¹⁹ especially its Articles 5 (data protection principles), Article 6 (lawfulness) and Article 9 (special categories of data),²⁰ the data exporter shall also comply with Chapter V (data transfers).²¹

將個人資料傳輸至非歐洲經濟區國家或國際組織時，除應遵守GDPR之相關規定¹⁹，特別是第5條（資料保護原則）、第6條（合法性）和第9條（特種個資）²⁰，資料輸出者還應遵守第五章（資料傳輸）之規範²¹。

60. In addition to the regular transparency requirement as mentioned on page 7 of the present guidelines, a duty rests on the data exporter to inform data subjects that it intends to transfer personal data to a third country or international organisation. This includes information about the existence or absence of an adequacy decision by the European Commission, or whether the transfer is based on a suitable safeguard from Article 46 or on a derogation of Article 49 (1). This duty exists irrespective of whether the personal data was obtained directly from the data subject or not.

除本指引第7頁(譯註：即本翻譯文件第15頁)論及之一般性透明化要求外，資料輸出者還有義務告知當事人，其有意將個人資料傳輸至

¹⁹ Article 44 GDPR.
GDPR第44條。

²⁰ See sections 4 to 6 of the present Guidelines.
見本指引第4節至第6節。

²¹ See the Guidelines 2/018 of the EDPB from 25.5.2018 on derogations of Article 49 under Regulation 2016/679, page 3, on the two-step test, available at https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en.
見EDPB 2018年5月25日「關於第2016/679號規則第49條的例外情形之指引2/2018（譯註：原文2/018應為誤植）」，頁3，二階段測試，請參閱：https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en。

第三國或國際組織。告知資訊包括歐盟執委會是否曾就其適足性作出認定，或傳輸是否具有第46條規定的適當安全維護措施或第49條第1項規定的例外。無論個人資料是否直接從當事人取得，都負有此一義務。

61. In general, when considering how to address such conditions for transfers of personal data to third countries or international organisations, data exporters should assess the risks to the rights and the freedoms of data subjects of each transfer²² and favour solutions that guarantee data subjects the continuous protection of their fundamental rights and safeguards as regards the processing of their data, even after it has been transferred. This will be the case for transfers to countries having an adequate level of protection,²³ or in case of use of one of the appropriate safeguards included in Article 46 GDPR,²⁴ ensuring that enforceable rights and effective legal remedies are available for data subjects.

一般而言，考量如何處理個人資料傳輸至第三國或國際組織的條件時，資料輸出者應評估每次傳輸對當事人權利和自由之風險²²，並優先選擇保證對於當事人之資料運用，即使在傳輸後，仍可持續保護當事人基本權利及安全維護措施之方案。例如傳輸目的國具備適足保護程度²³，或採用GDPR第46條²⁴規定的適當安全維護措施之一，從而確保當事人享有可依法行使之權利和有效法律救濟。

62. In the absence of an adequacy decision pursuant to Article 45 (3) GDPR

²² International Data Transfers may be a risk factor to consider when performing a DPIA as referred to in page 10 of the present guidelines.

實施本指引第10頁(譯註：即本翻譯文件第24頁)所述之個資保護影響評估時，國際資料傳輸可能是需考量的風險因素。

²³ The list of countries recognised adequate by the European Commission Link is available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

關於歐盟執委會認定之適足保護國家清單，請參閱：https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en。

²⁴ For example standard data protection clauses pursuant to Article 46 (2) (c) or (d) GDPR, ad hoc contractual clauses pursuant to Article 46 (3) (a) GDPR or administrative arrangements pursuant to Article 46 (3) (b) GDPR.

如GDPR第46條第2項第c款或第d款規定之標準資料保護條款，GDPR第46條第3項第a款規定之個案專用（ad hoc）契約條款，或GDPR第46條第3項第b款規定之行政安排。

or appropriate safeguards pursuant to Article 46 GDPR, Article 49 GDPR envisages certain specific situations under which transfers of personal data can take place as an exception. The derogations enshrined in Article 49 GDPR are thus exemptions from the general rule and, therefore, must be interpreted restrictively, and on a case-by-case basis.²⁵ Applied to the current COVID-19 crisis, those addressed in Article 49 (1) (d) (“transfer necessary for important reasons of public interest”) and (a) (“explicit consent”) may apply.

若欠缺GDPR第45條第3項規定的適足性認定，或GDPR第46條規定之適當安全維護措施，GDPR第49條規定得在特定情形下，例外進行個人資料傳輸。因此，GDPR第49條所列之例外情形，為一般原則之豁免，應根據個案具體情形，予以限縮解釋²⁵。對於當前的新冠肺炎危機，可能適用第49條第1項第d款（「基於公共利益之重要原因所為之必要傳輸」）及第a款（「明確同意」）。

63. The COVID-19 pandemic causes an exceptional sanitary crisis of an unprecedented nature and scale. In this context, the EDPB considers that the fight against COVID-19 has been recognised by the EU and most of its Member States as an important public interest,²⁶ which may require urgent action in the field of scientific research (for example to identify treatments and/or develop vaccines), and may also involve transfers to third countries or international organisations.²⁷

新冠肺炎疫情為一場性質與規模皆前所未見的嚴重衛生危機。在此情形下，EDPB認為，對抗新冠肺炎係歐盟及其大多數會員國所承認之重要公共利益²⁶，這可能需要科學研究領域迅速採取行動（如確定

²⁵ See Guidelines 2/2018, page 3.
見「2/2018指引」，頁3。

²⁶ Article 168 of the Treaty on the Functioning of the European Union recognises a high level of human health protection as an important objective that should be ensured in the implementation of all Union policies and activities. On this basis, Union action supports national policies to improve public health, including in combatting against major health scourges and serious cross-border threats to health, e.g. by promoting research into their causes, transmission and prevention. Similarly, Recitals 46 and 112 of the GDPR refer to processing carried out in the context of the fight against epidemics as an example of processing serving important grounds of public interest. In the context of the COVID-19 pandemic, the EU has adopted a series of measures in a broad range of areas (e.g. funding of healthcare systems, support to cross-border patients and deployment of medical staff, financial assistance to the most

治療方法和（或）開發疫苗），也可能涉及向第三國或國際組織傳輸資料²⁷。

64. Not only public authorities, but also private entities playing a role in pursuing such public interest (for example, a university's research institute cooperating on the development of a vaccine in the context of an international partnership) could, under the current pandemic context, rely upon the derogation mentioned above.

當前疫情期間，除公務機關外，追求此等公共利益之私人實體（如與國際夥伴合作開發疫苗的大學研究機構），亦仰賴前開之例外。

65. In addition, in certain situations, in particular where transfers are performed by private entities for the purpose of medical research aiming at fighting the COVID-19 pandemic,²⁸ such transfers of personal data could alternatively take place on the basis of the explicit consent of the data subjects.²⁹

此外，於特定情形下，特別是為對抗新冠肺炎疫情之相關醫學研究目的，由私人實體進行傳輸時²⁸，此種個人資料之傳輸亦可能以當事人之明確同意為依據²⁹。

66. Public authorities and private entities may, under the current pandemic

deprived, transport, medical devices etc.) premised on the understanding that the EU is facing a major public health emergency requiring an urgent response.

人類健康之高水準保護係歐盟運作條約第168條認可之重要目標，在實施歐盟各項政策與活動時，皆應確保符合這一目標。因此，歐盟活動支持促進公共衛生之國家政策，包括對抗重大健康危害和嚴重跨境之健康威脅之政策，如增進對其起因、傳播和防範方法之研究。同樣地，GDPR前言第46點和第112點提及，對抗流行病之相關運用，是為重要公共利益服務而運用之示例。新冠肺炎防疫期間，基於歐盟正面臨嚴峻公共衛生危機且需要迅速回應之認知，歐盟在諸多領域廣泛採取了一系列措施（如資助健康照護體系、支援跨境病患和部署醫療人員、向最弱勢群體提供經濟援助、運輸、醫療設備等）。

²⁷ The EDPB underlines that the GDPR, in its Recital 112, refers to the international data exchange between services competent for public health purposes as an example of the application of this derogation.

EDPB強調，GDPR前言第112點以適格公共衛生服務間的國際資料交換為例，說明了此一例外之適用。

²⁸ In accordance with Article 49 (3) GDPR, consent cannot be used for activities carried out by public authorities in the exercise of their public powers.

依GDPR第49條第3項，公務機關行使其公權力時，不得以同意為依據。

²⁹ See EDPB Guidelines 2/2018, section 2.1.

見EDPB「2/2018指引」，第2.1節。

context, when it is not possible to rely on an adequacy decision pursuant to Article 45 (3) or on appropriate safeguards pursuant to Article 46, rely upon the applicable derogations mentioned above, mainly as a temporary measure due to the urgency of the medical situation globally.

當前疫情狀況下，若無法依據GDPR第45條第3項規定的適足性認定，或GDPR第46條規定之適當安全維護措施，公務機關和私人實體得援用前開例外，主要將其作為當前全球緊急醫療狀態下的臨時措施。

67. Indeed, if the nature of the COVID-19 crisis may justify the use of the applicable derogations for initial transfers carried out for the purpose of research in this context, repetitive transfers of data to third countries part of a long lasting research project in this regard would need to be framed with appropriate safeguards in accordance with Article 46 GDPR.³⁰

事實上，若新冠肺炎危機得做為適用該項例外，為相關研究目的進行初次傳輸之正當化理由，則作為持續進行中的研究計畫之一部分，後續多次向第三國傳輸資料之行為，須採取GDPR第46條規定的適當安全維護措施³⁰。

68. Finally, it has to be noted that any such transfers will need to take into consideration on a case-by-case basis the respective roles (controller, processor, joint controller) and related obligations of the actors involved (sponsor, investigator) in order to identify the appropriate measures for framing the transfer.

最後，應注意，一切傳輸皆應依據個案情形，考量（控管者、受託運用者、共同控管者的）各自角色，以及所涉行動者（贊助者、調查員）之相關義務，以確定建構該項傳輸之適當措施。

³⁰ See EDPB Guidelines 2/2018, page 5.
見EDPB「2/2018指引」，頁5。

8. SUMMARY

結論

69. The key findings of these guidelines are:

本指引之主要結論如下：

1. The GDPR provides special rules for the processing of health data for the purpose of scientific research that are also applicable in the context of the COVID-19 pandemic.

為科學研究目的運用健康資料，GDPR定有特殊規範，此等規範亦適用於當前新冠肺炎疫情狀況。

2. The national legislator of each Member State may enact specific laws pursuant to Article (9) (2) (i) and (j) GDPR to enable the processing of health data for scientific research purposes. The processing of health data for the purpose of scientific research must also be covered by one of the legal bases in Article 6 (1) GDPR. Therefore, the conditions and the extent for such processing varies depending on the enacted laws of the particular member state.

各會員國的國家立法者得依據GDPR第9條第2項第i款和第j款制定具體法律，允許為科學研究目的運用健康資料。為科學研究目的運用健康資料，須具有GDPR第6條第1項規定之法律依據之一。因此，此種運用之條件與程度依具體會員國所制定之法律而有所不同。

3. All enacted laws based on Article (9) (2) (i) and (j) GDPR must be interpreted in the light of the principles pursuant to Article 5 GDPR and in consideration of the jurisprudence of the ECJ. In particular, derogations and limitations in relation to the protection of data provided in Article 9 (2) (j) and Article 89 (2) GDPR must apply only in so far as is strictly necessary.

依GDPR第9條第2項第i款和第j款制定之各項法律，其解釋須符合GDPR第5條之各項原則，且考量歐洲法院的實務見解。特別是，GDPR第9條第2項第j款和第89條第2項關於個資保護之例外與限制

規定，須以絕對必要為限。

4. Considering the processing risks in the context of the COVID-19 outbreak, high emphasise must be put on compliance with Article 5 (1) (f), Article 32 (1) and Article 89 (1) GDPR. There must be an assessment if a DPIA pursuant to Article 35 GDPR has to be carried out.

考量新冠肺炎疫情期間資料運用之風險，須著重強調遵守GDPR第5條第1項第f款、第32條第1項和第89條第1項規定。須評估是否應依GDPR第35條規定辦理個資保護影響評估。

5. Storage periods (timelines) shall be set and must be proportionate. In order to define such storage periods, criteria such as the length and the purpose of the research should be taken into account. National provisions may stipulate rules concerning the storage period as well and must therefore be considered.

應設定合乎比例之儲存期間（時限）。為確定儲存期間，應考慮研究之時間長度和目的等標準。國家法律亦可能包含儲存期間相關規定，此等規定亦須予以考慮。

6. In principle, situations as the current COVID-19 outbreak do not suspend or restrict the possibility of data subjects to exercise their rights pursuant to Article 12 to 22 GDPR. However, Article 89 (2) GDPR allows the national legislator to restrict (some) of the data subject's rights as set in Chapter 3 of the GDPR. Because of this, the restrictions of the rights of data subjects *may vary* depending on the enacted laws of the particular Member State.

原則上，當前新冠肺炎疫情等狀況不會中止或限制當事人依GDPR第12條至第22條行使權利。然而，GDPR第89條第2項允許國家立法者限制當事人依GDPR第三章享有的（某些）權利。因此，對當事人權利之限制，可能因具體會員國所制定之法律而有所不同。

7. With respect to international transfers, in the absence of an adequacy decision pursuant to Article 45 (3) GDPR or appropriate safeguards pursuant to Article 46 GDPR, public authorities and private entities may rely upon the applicable derogations pursuant to Article 49 GDPR. However, the derogations of Article 49 GDPR do have exceptional character only.

國際傳輸方面，若欠缺GDPR第45條第3項規定的適足性認定，或GDPR第46條規定之適當安全維護措施，公務機關和私人實體得援用GDPR第49條之例外條款。但此GDPR第49條之例外條款僅得例外適用。

For the European Data Protection Board

The Chair

(Andrea Jelinek)

歐盟個人資料保護委員會

主席

(Andrea Jelinek)

Guidelines



**Guidelines 2/2019 on the processing of personal data
under Article 6(1)(b) GDPR in the context of the
provision of online services to data subjects**

**關於向當事人提供線上服務時依GDPR第6條第1項第
b款運用個人資料之指引2/2019**

**Version 2.0
版本2.0**

**8 October 2019
2019年10月8日**

Version history

版本更新歷程

Version 2.0 版本 2.0	8 October 2019 2019年10月8日	Adoption of the Guidelines after public consultation 公眾諮詢後通過本指引
Version 1.0 版本 1.0	9 April 2019 2019年4月9日	Adoption of the Guidelines for publication consultation 通過本指引供公眾諮詢

1	Part 1 – Introduction 第1部分—導言	4
1.1	Background 背景	4
1.2	Scope of these guidelines 本指引之範圍	8
2	Part 2 - Analysis of Article 6(1)(b) 第2部分—第6條第1項第b款之分析	9
2.1	General observations 一般意見	9
2.2	Interaction of Article 6(1)(b) with other lawful bases for processing 第6條第1項第b款與其他運用之合法依據之關係	12
2.3	Scope of Article 6(1)(b) 第6條第1項第b款之範圍	14
2.4	Necessity 必要性.....	15
2.5	Necessary for performance of a contract with the data subject 為履行與當事人間契約所必要.....	17
2.6	Termination of contract 契約之終止	25
2.7	Necessary for taking steps prior to entering into a contract 為締約前採取步驟所必要.....	28
3	Part 3 – Applicability of Article 6(1)(b) in specific situations 第3部分—特定情境中第6條第1項第b款之可適用性	30
3.1	Processing for ‘service improvement’ 為「改進服務」而運用	30
3.2	Processing for ‘fraud prevention’ 為「防範詐欺」而運用	31
3.3	Processing for online behavioural advertising 為線上行為廣告而運用	31
3.4	Processing for personalisation of content 為個人化內容而運用	34

The European Data Protection Board

Having regard to Article 70(1)e of Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

HAS ADOPTED THE FOLLOWING GUIDELINES

歐盟個人資料保護委員會

依據歐洲議會與歐盟理事會於2016年4月27日通過之「關於運用*個人資料時對自然人之保護與確保此等資料之自由流通，以及廢除指令95/46/EC的歐盟規則2016/679/EU」第70條第1項第e款，

通過以下指引：

1 PART 1 – INTRODUCTION

第1部分—導言

1.1 Background

背景

1. Pursuant to Article 8 of the Charter of Fundamental Rights of the European Union, personal data must be processed fairly for specified purposes and on the basis of a legitimate basis laid down by law. In this regard, Article 6(1) of the General Data Protection Regulation¹ (GDPR) specifies that processing shall be lawful only on the basis of one of six specified conditions set out in Article 6(1)(a) to (f). Identifying the appropriate legal basis that corresponds to the objective and essence of the processing is of essential importance. Controllers must, *inter alia*,

* 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」。

take into account the impact on data subjects' rights when identifying the appropriate lawful basis in order to respect the principle of fairness.

依據「歐洲聯盟基本權利憲章」第8條，個人資料之運用應為特定目的，基於法定之正當依據，以公平合理方式為之。在此方面，「一般資料保護規則」¹（GDPR）第6條第1項明確規定，唯有以第6條第1項第a款至第f款規定之六項條件為依據時，運用方為合法。依據運用之目標與本質，識別適當的法律依據，為核心重要事項。確認適當合法依據以求符合公平合理原則時，控管者須尤其（*inter alia*）考量對當事人權利之影響。

2. Article 6(1)(b) GDPR provides a lawful basis for the processing of personal data to the extent that “processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”.² This supports the freedom to conduct a business, which is guaranteed by Article 16 of the Charter, and reflects the fact that sometimes the contractual obligations towards the data subject cannot be performed without the data subject providing certain personal data. If the specific processing is part and parcel of delivery of the requested service, it is in the interests of both parties to process that data, as otherwise the service could not be provided and the contract could not be performed. However, the ability to rely on this or one of the other legal bases mentioned in Article 6(1) does not exempt the controller from compliance with the other requirements of the GDPR.

GDPR第6條第1項第b款規定了一項個人資料運用之合法依據，即「運用係為履行當事人所立契約所必要，或係締約前應當事人之要求採取步驟所必要」²。本條支持「憲章」第16條所保障之營業自由，且反映出一項事實，即某些情況下，若當事人不提供特定個人資料，則無法對其履行契約義務。若特定運用行為是提供所請求之服務的必要部分，則運用此等資料符合契約雙方的利益，因為若非如此，

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

歐洲議會與歐盟理事會於2016年4月27日通過之「關於運用個人資料時對自然人之保護與確保此等資料之自由流通，以及廢除指令95/46/EC的歐盟規則(EU) 2016/679」（一般資料保護規則）。

² See also recital 44.

另見前言第44點。

將無法提供服務，亦無法履行契約。然而，援用本款或第6條第1項所述的其他法律依據，並不免除控管者遵守GDPR其他要求之義務。

3. Articles 56 and 57 of the Treaty on the Functioning of the European Union define and regulate the freedom to provide services within the European Union. Specific EU legislative measures have been adopted in respect of ‘information society services’.³ These services are defined as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.” This definition extends to services that are not paid for directly by the persons who receive them,⁴ such as online services funded through advertising. ‘Online services’ as used in these guidelines refers to ‘information society services’.

「歐洲聯盟運作條約」第56條和第57條定義並規範歐盟境內提供服務之自由。對於「資訊社會服務」（information society services），已採取具體歐盟立法措施³。此等服務被定義為「通常收取報酬、遠距、以電子方式且應服務接收者個別請求而提供之任何服務。」此一定義涵蓋非由服務接收者直接付費的服務⁴，如透過廣告獲得收入的線上服務。本指引所述之「線上服務」係指「資訊社會服務」。

4. The development of EU law reflects the central importance of online services in modern society. The proliferation of always-on mobile internet and the widespread availability of connected devices have enabled the development of online services in fields such as social media, e-commerce, internet search, communication, and travel. While some of these services are funded by user payments, others are provided without monetary payment by the consumer, instead financed by the sale of online advertising services allowing for targeting of data subjects. Tracking of user behaviour for the purposes of such advertising is often carried out in ways the user is often not aware of,⁵ and it may not be

³ See for example Directive (EU) 2015/1535 of the European Parliament and of the Council, and Article 8 GDPR.

示例見歐洲議會與歐盟理事會之指令(EU) 2015/1535，以及GDPR第8條。

⁴ See Recital 18 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

見歐洲議會與歐盟理事會於2000年6月8日通過之「關於內部市場中資訊社會服務之特定法律面向，特別是電子商務的歐盟指令2000/31/EC」前言第18點。

immediately obvious from the nature of the service provided, which makes it almost impossible in practice for the data subject to exercise an informed choice over the use of their data.

歐盟法之發展反映出線上服務在現代社會中的核心重要性。藉助始終連線（always-on）的移動網路之激增與聯網裝置之普及，社群媒體、電子商務、網路搜尋、通訊和旅遊等領域的線上服務得以發展。雖然其中一些服務是透過使用者付費獲得收入，其他服務之提供則不向消費者收費，而是透過銷售能夠對當事人定向投放之線上廣告服務獲得收入。為此等廣告目的對使用者行為之追蹤，通常以使用者並不知情之方式實施⁵，且可能無法從所提供服務之性質立即呈現出來，因此使得當事人在實際上幾乎不可能就其資料之利用進行知情選擇。

5. Against this background, the European Data Protection Board⁶ (EDPB) considers it appropriate to provide guidance on the applicability of Article 6(1)(b) to processing of personal data in the context of online services, in order to ensure that this lawful basis is only relied upon where appropriate.

在此背景下，歐盟個人資料保護委員會⁶（EDPB）認為，宜就第6條第1項第b款對線上服務所涉個人資料運用之適用性提供指導，以確保僅於適當時援用此一合法依據。

6. The Article 29 Working Party (WP29) has previously expressed views on the contractual necessity basis under Directive 95/46/EC in its opinion on the notion of legitimate interests of the data controller.⁷ Generally, that guidance remains relevant to Article 6(1)(b) and the GDPR.

第29條工作小組（WP29）在其關於資料控管者正當利益概念之意見中，曾就指令95/46/EC規定的契約必要性依據發表見解⁷。一般而言，該指導對於第6條第1項第b款和GDPR仍具有相關性。

⁵ In this regard, controllers need to fulfil the transparency obligations set out in the GDPR.

在此方面，控管者需履行GDPR規定之透明化義務。

⁶ Established under Article 68 GDPR.

依GDPR第68條設立。

⁷ Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217). See in particular pages 11, 16, 17, 18 and 55.

第29條工作小組「關於指令95/46/EC第7條之資料控管者正當利益概念之意見06/2014」（WP217）。尤其參見頁11、16、17、18和55。

1.2 Scope of these guidelines

本指引之範圍

7. These guidelines are concerned with the applicability of Article 6(1)(b) to processing of personal data in the context of contracts for online services, irrespective of how the services are financed. The guidelines will outline the elements of lawful processing under Article 6(1)(b) GDPR and consider the concept of 'necessity' as it applies to 'necessary for the performance of a contract'.

本指引係關於第6條第1項第b款對於線上服務契約所涉個人資料運用行為之適用性，而無論該等服務如何獲取收入。本指引將闡述GDPR第6條第1項第b款之合法運用要件，並討論「為履行契約所必要」中「必要」之含義。

8. Data protection rules govern important aspects of how online services interact with their users, however, other rules apply as well. Regulation of online services involves cross-functional responsibilities in the fields of, *inter alia*, consumer protection law, and competition law. Considerations regarding these fields of law are beyond the scope of these guidelines.

資料保護規則規範線上服務與使用者互動之重要事項，然而，其他規則亦有其適用。線上服務之規範涉及跨部會（跨功能）之職責，特別是消費者保護法與競爭法領域。這些領域之考量已超出本指引之範圍。

9. Although Article 6(1)(b) can only apply in a contractual context, these guidelines do not express a view on the validity of contracts for online services generally, as this is outside the competence of the EDPB. Nonetheless, contracts and contractual terms must comply with the requirements of contract laws and, as the case may be for consumer contracts, consumer protection laws in order for processing based on those terms to be considered fair and lawful.

雖然第6條第1項第b款僅適用於契約，本指引並不對線上服務契約之一般有效性表達見解，因為這已超出EDPB的職權範圍。然而，契約及契約條款須符合契約法，消費者契約還須符合消費者保護法，基於其條款之運用方可被視為公平且合法。

10. Some general observations on data protection principles are included

below, but not all data protection issues that may arise when processing under Article 6(1)(b) will be elaborated on. Controllers must always ensure that they comply with the data protection principles set out in Article 5 and all other requirements of the GDPR and, where applicable, the ePrivacy legislation.

下列內容包含資料保護原則的一般觀察，但不會對依第6條第1項第b款運用資料所涉之一切資料保護議題均作詳細說明。控管者必須確保遵守第5條規定的資料保護原則、GDPR的其他要求，以及在適用時，遵守電子隱私規範。

2 PART 2 - ANALYSIS OF ARTICLE 6(1)(B)

第2部分—第6條第1項第b款之分析

2.1 General observations

一般意見

11. The lawful basis for processing on the basis of Article 6(1)(b) needs to be considered in the context of the GDPR as a whole, the objectives set out in Article 1, and alongside controllers' duty to process personal data in compliance with the data protection principles pursuant to Article 5. This includes processing personal data in a fair and transparent manner and in line with the purpose limitation and data minimisation obligations.

以第6條第1項第b款為合法依據之運用，需考量GDPR整體、第1條規定之目標，以及控管者依第5條規定的資料保護原則運用個人資料之義務。這包括以公平合理及透明之方式運用個人資料，並符合目的限制與資料最小化義務。

12. Article 5(1)(a) GDPR provides that personal data must be processed lawfully, fairly and transparently in relation to the data subject. The principle of fairness includes, inter alia, recognising the reasonable expectations⁸ of the data subjects, considering possible adverse consequences processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller.

GDPR第5條第1項第a款規定，個人資料之運用須以合法、公平合理和並對當事人以透明之方式為之。公平合理原則尤其包括識別當事人

之合理期待⁸，考量運用對其可能造成的不利影響，並顧及其與控管者間之關係，以及不對等關係之潛在影響。

13. As mentioned, as a matter of lawfulness, contracts for online services must be valid under the applicable contract law. An example of a relevant factor is whether the data subject is a child. In such a case (and aside from complying with the requirements of the GDPR, including the ‘specific protections’ which apply to children),⁹ the controller must ensure that it complies with the relevant national laws on the capacity of children to enter into contracts. Furthermore, to ensure compliance with the fairness and lawfulness principles, the controller needs to satisfy other legal requirements. For example, for consumer contracts, Directive 93/13/EEC on unfair terms in consumer contracts (the “Unfair Contract Terms Directive”) may be applicable.¹⁰ Article 6(1)(b) is not limited to contracts governed by the law of an EEA member state.¹¹

如前所述，合法性方面，線上服務契約依所適用之契約法須為有效。相關因素之一個示例為當事人是否為兒童。此時（在遵守GDPR之要求，包括適用於兒童之「特別保護」要求的同時）⁹，控管者必須確保遵守兒童締約能力相關的國內法律。此外，為確保遵守公平合理與合法性原則，控管者須滿足其他法律要求。例如，對於消費者契約，可能適用關於消費者契約中不公平條款之歐盟指令93/13/EEC（「不公平契約條款指令」）¹⁰。第6條第1項第b款並不限於受歐洲

⁸ Some personal data are expected to be private or only processed in certain ways, and data processing should not be surprising to the data subject. In the GDPR, the concept of ‘reasonable expectations’ is specifically referenced in recitals 47 and 50 in relation to Article 6(1)(f) and (4).

某些個人資料被期待為私密性質或僅得以特定方式運用，資料運用不應使當事人感到意外。GDPR中，「合理期待」之概念在前言第47點和第50點中被特別提及，此兩點係關於第6條第1項第f款和第4項。

⁹ See Recital 38, which refers to children meriting 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.

見前言第38點，該點提到，兒童之個人資料需要特別保護，因為兒童可能對個人資料運用所涉之風險、後果、安全維護措施及其權利的認知較低。

¹⁰ A contractual term that has not been individually negotiated is unfair under the Unfair Contract Terms Directive “if, contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations arising under the contract, to the detriment of the consumer”. Like the transparency obligation in the GDPR, the Unfair Contract Terms Directive mandates the use of plain, intelligible language. Processing of personal data that is based on what is deemed to be an unfair term under the Unfair Contract Terms Directive, will generally not be consistent with the requirement under Article 5(1)(a) GDPR that processing is lawful and fair.

依不公平契約條款指令，若未經個別磋商的契約條款「違反善意要求，造成雙方間的契約權利

經濟區會員國法律管轄之契約¹¹。

14. Article 5(1)(b) of the GDPR provides for the purpose limitation principle, which requires that personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

GDPR第5條第1項第b款規定了目的限制原則，該原則要求個人資料之蒐集須有特定、明確且正當之目的，且不得以該等目的不相容之方式為進階運用。

15. Article 5(1)(c) provides for data minimisation as a principle, i.e. processing as little data as possible in order to achieve the purpose. This assessment complements the necessity assessments pursuant to Article 6(1)(b) to (f).

GDPR第5條第1項第c款已規定資料最小化原則，亦即，盡可能運用最少量的資料以達成目的。該資料最小化評估補充了第6條第1項第b款至第f款的必要性評估。

16. Both purpose limitation and data minimisation principles are particularly relevant in contracts for online services, which typically are not negotiated on an individual basis. Technological advancements make it possible for controllers to easily collect and process more personal data than ever before. As a result, there is an acute risk that data controllers may seek to include general processing terms in contracts in order to maximise the possible collection and uses of data, without adequately specifying those purposes or considering data minimisation obligations. WP29 has previously stated:

目的限制和資料最小化原則皆與線上服務契約尤其相關，此等契約通常未經個別磋商。技術進步使得控管者能夠比以往更輕易蒐集並運用大量個人資料。因此，存在如下嚴峻風險：控管者可能試圖在契約中納入一般性運用條款，以盡可能擴大資料之蒐集與使用範圍，而不充分具體說明其目的或考量資料最小化義務。第29條工作小組

義務嚴重不對等，且對消費者不利」，則該條款係不公正。與GDPR中的透明化義務類似，不公平契約條款指令要求使用平實易懂之語言。若個人資料之運用係以不公平契約條款指令所規定之不公平條款為依據，則其運用一般不符合GDPR第5條第1項第a款運用應合法且公平合理之要求。

¹¹ The GDPR applies to certain controllers outside the EEA; see Article 3 GDPR. GDPR適用於位於歐洲經濟區外的特定控管者，見GDPR第3條。

曾說明：

The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied. For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'.¹²

必須明確具體地說明蒐集之目的：說明須足夠詳盡，以判斷何種運用係包含在該特定目的範圍內、何種運用係在該範圍之外，並應足以評估法律遵循狀況、適用資料保護安全維護措施。因此，模糊寬泛且未說明細節之目的，如「提升使用者體驗」、「行銷目的」、「信息技術目的」或「未來研究目的」等，通常不符「特定性」標準¹²。

2.2 Interaction of Article 6(1)(b) with other lawful bases for processing

第6條第1項第b款與其他運用之合法依據之關係

17. Where processing is not considered 'necessary for the performance of a contract', i.e. when a requested service can be provided without the specific processing taking place, the EDPB recognises that another lawful basis may be applicable, provided the relevant conditions are met. In particular, in some circumstances it may be more appropriate to rely on freely given consent under Article 6(1)(a). In other instances, Article 6(1)(f) may provide a more appropriate lawful basis for processing. The legal basis must be identified at the outset of processing, and information given to data subjects in line with Articles 13 and 14 must specify the legal basis.

若運用不構成「履行契約所必要」，亦即，若所請求之服務無需特定運用即可提供，EDPB認為，在滿足相關條件的情況下，可能適用其他合法依據。特別地，某些情況下，可能更宜適用第6條第1項第a

¹² Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), page 15–16.
第29條工作小組「關於目的限制之意見03/2013」（WP203），頁15-16。

款規定之自由給予之同意。其他情形下，第6條第1項第f款可能為運用提供更為適宜的合法依據。必須在運用初始即識別法律依據，且依第13條和第14條告知當事人之資訊必須明確其法律依據。

18. It is possible that another lawful basis than Article 6(1)(b) may better match the objective and context of the processing operation in question. The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation.¹³

第6條第1項第b款以外的其他合法依據可能更符合所涉運用之目的與情況。識別適當合法目的，與公平合理原則及目的限制密切相關¹³。

19. The WP29 guidelines on consent also clarify that where “a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis”. Conversely, the EDPB considers that where processing is not in fact necessary for the performance of a contract, such processing can take place only if it relies on another appropriate legal basis.¹⁴

第29條工作小組關於同意之指引亦釐清，「如控管者有意運用事實上係為履行契約所必要的個人資料，則同意即非適當的合法依據」。反之，EDPB認為，若運用事實上並非為履行契約所必要，則惟有援用其他適當之法律依據時，方得實施此等運用¹⁴。

20. In line with their transparency obligations, controllers should make sure to avoid any confusion as to what the applicable legal basis is. This is particularly relevant where the appropriate legal basis is Article 6(1)(b) and a contract regarding online services is entered into by data subjects. Depending on the circumstances, data subjects may erroneously get the impression that they are giving their consent in line with Article 6(1)(a) when signing a contract or accepting terms of service. At the same time, a controller might erroneously assume that the signature of a contract

¹³ When controllers set out to identify the appropriate legal basis in line with the fairness principle, this will be difficult to achieve if they have not first clearly identified the purposes of processing, or if processing personal data goes beyond what is necessary for the specified purposes.

控管者依公平合理原則識別適當法律依據時，若其未首先明確運用之目的，或若個人資料之運用超出特定目的所必要之範圍，則將很難符合公平合理原則。

¹⁴ For more information on implications in relation to Article 9, see Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259), endorsed by the EDPB, pages 19–20.

關於第9條相關影響的更多資訊，見第29條工作小組「關於第2016/679號規則（GDPR）中的同意之指引」（WP259），EDPB採認，頁19-20。

corresponds to a consent in the sense of article 6(1)(a). These are entirely different concepts. It is important to distinguish between accepting terms of service to conclude a contract and giving consent within the meaning of Article 6(1)(a), as these concepts have different requirements and legal consequences.

為遵守其透明化義務，控管者須確保避免混淆所適用之法律依據。若以第6條第1項第b款為適當法律依據且與當事人訂立線上服務契約時，這一點尤為重要。根據具體情況，當事人可能錯誤地以為其在簽訂契約或接受服務條款時，係在依第6條第1項第a款給予同意。與此同時，控管者可能錯誤地以為，簽訂契約即等同第6條第1項第a款意義上之同意。此為完全不同之概念。重要的是區分接受服務條款以訂立契約，以及給予第6條第1項第a款之同意，因為這些概念有不同的要求與法律效果。

21. In relation to the processing of special categories of personal data, in the guidelines on consent, WP29 has also observed that:

關於運用特種個資，第29條工作小組在同意指引中說明：

*Article 9(2) does not recognize ‘necessary for the performance of a contract’ as an exception to the general prohibition to process special categories of data. Therefore controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). Should none of the exceptions (b) to (j) apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data.*¹⁵

第9條第2項未將「為履行契約所必要」列為禁止運用特種個資之例外。因此控管者及會員國對此應探究第9條第2項第b款至第j款的特殊例外規定。若第b款至第j款均不適用時，遵守GDPR對有效同意之條件以獲得明確同意，將成為運用該類個資唯一可能的合法例外¹⁵。

2.3 Scope of Article 6(1)(b)

第6條第1項第b款之範圍

¹⁵ Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259), endorsed by the EDPB, page 19.

第29條工作小組「關於第2016/679號規則（GDPR）中的同意之指引」（WP259），EDPB採認，頁19。

22. Article 6(1)(b) applies where either of two conditions are met: the processing in question must be objectively necessary for the performance of a contract with a data subject, or the processing must be objectively necessary in order to take pre-contractual steps at the request of a data subject.

滿足如下兩個條件之一時，適用第6條第1項第b款：運用必須係為履行與當事人間契約所客觀必要，或運用係應當事人之要求採取締約前步驟所客觀必要。

2.4 Necessity

必要性

23. Necessity of processing is a prerequisite for both parts of Article 6(1)(b). At the outset, it is important to note that the concept of what is 'necessary for the performance of a contract' is not simply an assessment of what is permitted by or written into the terms of a contract. The concept of necessity has an independent meaning in European Union law, which must reflect the objectives of data protection law.¹⁶ Therefore, it also involves consideration of the fundamental right to privacy and protection of personal data,¹⁷ as well as the requirements of data protection principles including, notably, the fairness principle.

運用之必要性係第6條第1項第b款兩個部分共同之必要條件。首先須注意，「係為履行契約所必要」之概念並非契約條款允許或明定哪些事項之簡單判斷。必要性之概念在歐盟法中有獨立含義，且必須反映資料保護法之目的¹⁶。因此，其亦涉及考量隱私與個人資料保護之基本權利¹⁷，以及資料保護原則（其中尤其包括公平合理原則）之要求。

24. The starting point is to identify the purpose for the processing, and in the

¹⁶ The CJEU stated in *Huber* that "what is at issue is a concept [necessity] which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of that Directive, [Directive 95/46], as laid down in Article 1(1) thereof". CJEU, Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, 18 December 2008, para. 52.

*Huber*案中，歐盟法院（CJEU）認為，「本案之問題是，一個概念（必要性）在共同體法律中有其獨立含義，且其解釋須充分反映該指令（指令95/46）第1條第1項規定之目的」。歐盟法院，第C-524/06號案件（*Heinz Huber v Bundesrepublik Deutschland*）判決，2008年12月16日（譯註：原文18日應為誤植），第52段。

¹⁷ See Articles 7 and 8 of the Charter of Fundamental Rights of the European Union 見「歐洲聯盟基本權利憲章」第7條和第8條。

context of a contractual relationship, there may be a variety of purposes for processing. Those purposes must be clearly specified and communicated to the data subject, in line with the controller's purpose limitation and transparency obligations.

首先應識別運用之目的。對於契約關係而言，可能存在諸多運用目的。須依據控管者的目的限制和透明化義務，明確說明這些目的，並告知當事人。

25. Assessing what is 'necessary' involves a combined, fact-based assessment of the processing "for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal".¹⁸ If there are realistic, less intrusive alternatives, the processing is not 'necessary'.¹⁹ Article 6(1)(b) will not cover processing which is useful but not objectively necessary for performing the contractual service or for taking relevant pre-contractual steps at the request of the data subject, even if it is necessary for the controller's other business purposes.

要判斷何為「必要」，須基於事實綜合評估，即評估「該運用之目的以及相較於其他可達成相同目的之選項，干預程度是否較低」¹⁸。若存在干預性更低的其他可行之替代方案，則運用並非「必要」¹⁹。

¹⁸ See EDPS Toolkit: Assessing the Necessity of Measures that limit the fundamental right to the protection of personal data, page 5.

見歐盟個人資料保護監察人（EDPS）工具庫（Toolkit）：「個人資料保護基本權利限制措施之必要性評估」，頁5。

¹⁹ In *Schecke*, the CJEU held that, when examining the necessity of processing personal data, the legislature needed to take into account alternative, less intrusive measures. CJEU, Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, 9. November 2010. This was repeated by the CJEU in the *Rīgas* case where it held that "As regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary". CJEU, Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, para. 30. A strict necessary test is required for any limitations on the exercise of the rights to privacy and to personal data protection with regard to the processing of personal data, see EDPS Toolkit: Assessing the Necessity of Measures that limit the fundamental right to the protection of personal data, page 7.

*Schecke*案中，歐盟法院認為，檢視個人資料運用之必要性時，立法機關需考量干預性更低的替代方案。歐盟法院，合併審理之第C-92/09號案件（*Volker und Markus Schecke GbR*）和第C-93/09號案件（*Hartmut Eifert v Land Hessen*）判決，2010年11月9日。*Rīgas*案中，歐盟法院再次重申此一見解，認為「關於個人資料運用必要性之相關條件，應謹記個人資料保護相關之例外與限制，其適用以絕對必要為限」。歐盟法院，第C-13/16號案件（*Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*）判決，第30段。對於個人資料運用行為行使隱私權和資料保護權之任何限制均需通過絕對必要測試，見EDPS工具庫：

若運用雖然實用，但對於提供契約服務或應當事人之要求採取相關締約前步驟而言並非客觀必要，則其並不涵蓋在第6條第1項第b款範圍內，即使該運用係為控管者的其他業務目的所必要。

2.5 Necessary for performance of a contract with the data subject 為履行與當事人間契約所必要

26. A controller can rely on the first option of Article 6(1)(b) to process personal data when it can, in line with its accountability obligations under Article 5(2), establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the *particular contract* with the data subject can be performed. Where controllers cannot demonstrate that (a) a contract exists, (b) the contract is valid pursuant to applicable national contract laws, and (c) that the processing is objectively necessary for the performance of the contract, the controller should consider another legal basis for processing.

若控管者能夠在遵守第5條第2項規定之課責性義務的情況下，同時確立運用係基於與當事人間之有效契約，以及運用係為履行與當事人間之該特定契約所必要，則其得援用第6條第1項第b款之第一個選項運用個人資料。若控管者無法證明（a）存在契約；（b）該契約依所適用之國內契約法係有效；且（c）運用係為履行該契約所客觀必要，則控管者應考慮運用之其他法律依據。

27. Merely referencing or mentioning data processing in a contract is not enough to bring the processing in question within the scope of Article 6(1)(b). On the other hand, processing may be objectively necessary even if not specifically mentioned in the contract. In any case, the controller must meet its transparency obligations. Where a controller seeks to establish that the processing is based on the performance of a contract with the data subject, it is important to assess what is *objectively necessary* to perform the contract. ‘Necessary for performance’ clearly requires something more than a contractual clause. This is also clear in light of Article 7(4). Albeit this provision only regards validity of consent, it illustratively makes a distinction between processing activities

「個人資料保護基本權利限制措施之必要性評估」，頁7。

necessary for the performance of a contract, and *clauses* making the service conditional on certain processing activities that are not in fact necessary for the performance of the contract.

僅在契約中涉及或提到資料運用並不足以使相關運用落入第6條第1項第b款之範圍內。另一方面，即使契約並未明確提及，運用也可能係客觀必要。無論如何，控管者必須遵守其透明化義務。若控管者有意確立運用係基於履行與當事人間之契約，則須評估哪些事項係為履行契約所客觀必要。「履行所必要」所要求的顯然不止契約條款。這在第7條第4項也有明確表現。雖然該條僅涉及同意之有效性，其示範性地區分了為履行契約所必要之運用活動，以及規定服務係以特定運用活動為條件（而運用事實上並非履行契約所必要）之契約條款。

28. In this regard, the EDPB endorses the guidance previously adopted by WP29 on the equivalent provision under the previous Directive that ‘necessary for the performance of a contract with the data subject’:

在此方面，EDBP採認第29條工作小組此前通過的關於先前「指令」中相當規定（equivalent provision）之指導，認為「為履行與當事人間契約所必要」：

... must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some processing is covered by a contract does not automatically mean that the processing is necessary for its performance. [...] Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them ‘necessary’ for the performance of the contract.²⁰

…必須嚴格解釋，且並不涵蓋運用並非真正為履行契約所必要，而是由控管者單方課加予當事人之情形。同時，契約涵蓋某種運用之事實，並不必然意味著運用係為履行契約所必要。…即使此等運用活動在契約中有明文規定，僅憑這一事實也並不使得運用係為履行契約所「必要」²⁰。

²⁰ Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), page 16–17.

第29條工作小組「關於指令95/46/EC第7條之資料控管者正當利益概念之意見06/2014」（WP217），頁16-17。

29. The EDPB also recalls the same WP29 guidance stating:

EDPB亦重申第29條工作小組同一指導之如下見解：

*There is a clear connection here between the assessment of necessity and compliance with the purpose limitation principle. It is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance.*²¹

必要性評估與遵守目的限制原則間有明確關聯。確定契約之確切意旨（*exact rationale*）很重要，亦即其本質與根本目標，因為這是審視資料運用是否為履行契約所必要之標準²¹。

30. When assessing whether Article 6(1)(b) is an appropriate legal basis for processing in the context of an online contractual service, regard should be given to the particular aim, purpose, or objective of the service. For applicability of Article 6(1)(b), it is required that the processing is *objectively necessary* for a purpose that is integral to the delivery of that contractual service to the data subject. Not excluded is processing of payment details for the purpose of charging for the service. The controller should be able to demonstrate how the main subject-matter of the *specific contract with the data subject* cannot, as a matter of fact, be performed if the specific processing of the *personal data in question* does not occur. The important issue here is the nexus between the personal data and processing operations concerned, and the performance or non-performance of the service provided under the contract.

評估第6條第1項第b款是否係提供線上契約服務時運用資料之適當法律依據，應考量該服務之特定目標、宗旨或目的。第6條第1項第b款之適用，要求運用係為向當事人提供契約服務不可或缺之目的所客觀必要。此未排除為收取服務費用而運用付款資料。控管者應能夠證明，若不運用相關個人資料，則與當事人間該特定契約之主要標的將如何在事實上無法履行。此處的要點是個人資料與運用活動間、以及與契約所涉服務之履行或不履行間的關聯。

31. Contracts for digital services may incorporate express terms that impose

²¹ Ibid., page 17.

同前註，頁17。

additional conditions about advertising, payments or cookies, amongst other things. A contract cannot artificially expand the categories of personal data or types of processing operation that the controller needs to carry out for the performance of the contract within the meaning of Article 6(1)(b).

數位服務契約可能包括廣告、付款或cookie等附加條件的明文條款。契約不可在第6條第1項第b款的規範意義外，刻意擴張控管者為履行契約所必須的個人資料類別或運用活動類型。

32. The controller should be able to justify the necessity of its processing by reference to the fundamental and mutually understood contractual purpose. This depends not just on the controller's perspective, but also a reasonable data subject's perspective when entering into the contract, and whether the contract can still be considered to be 'performed' without the processing in question. Although the controller may consider that the processing is necessary for the contractual purpose, it is important that they examine carefully the perspective of an average data subject in order to ensure that there is a genuine mutual understanding on the contractual purpose.

控管者應能夠援引雙方共同理解之契約根本目的，作為其運用必要性的正當化理由。這不僅取決於控管者的觀點，還包括理性當事人訂立契約時的觀點，以及如不進行相關運用，契約是否可視為已「履行」。即使控管者認為運用係為契約目的所必要，仍應仔細檢視一般當事人之觀點，以確保雙方對於契約目的有真正合意理解。

33. In order to carry out the assessment of whether Article 6(1)(b) is applicable, the following questions can be of guidance:

為評估第6條第1項第b款是否可適用，下列問題可提供指導：

- What is the nature of the service being provided to the data subject?
What are its distinguishing characteristics?
向當事人提供之服務之本質為何？其有哪些顯著特徵？
- What is the exact rationale of the contract (i.e. its substance and fundamental object)?
契約之確切意旨（亦即其本質與根本目標）為何？
- What are the essential elements of the contract?

契約的根本要素有哪些？

- What are the mutual perspectives and expectations of the parties to the contract? How is the service promoted or advertised to the data subject? Would an ordinary user of the service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?

契約雙方的共同觀點與期待有哪些？該服務是如何向當事人推銷或廣告？依該服務之本質，該服務的一般使用者身為契約當事人，可否合理期待將發生控管者為履行契約所預想的運用？

34. If the assessment of what is ‘necessary for the performance of a contract’, which must be conducted prior to the commencement of processing, shows that the intended processing goes beyond what is objectively necessary for the performance of a contract, this does not render such future processing unlawful per se. As already mentioned, Article 6 makes clear that other lawful bases are potentially available prior to the initiation of the processing.²²

何者「係為履行契約所必要」之評估必須在運用開始前為之，若此等評估表明有意實施之運用超出履行契約客觀必要之範圍，並不使得未來運用本身違法。如前所述，第6條已明確表示，開始運用前，其他合法依據可能有其適用²²。

35. If, over the lifespan of a service, new technology is introduced that changes how personal data are processed, or the service otherwise evolves, the criteria above need to be assessed anew to determine if any new or altered processing operations can be based on Article 6(1)(b).

在提供服務的過程中，若出現改變個人資料運用方式的新技術，或該服務發生其他演變，應重新評估上述標準，以確定新運用或改變後的運用活動能否以第6條第1項第b款為依據。

²² See Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259), endorsed by the EDPB, page 31, in which it is stated that: “Under the GDPR, it is not possible to swap between one lawful basis and another.”

見第29條工作小組「關於第2016/679號規則（GDPR）中的同意之指引」（WP259），EDPB採認，頁31，該工作小組認為「依GDPR，不得將某一合法依據替換為其他依據」。

Example 1

A data subject buys items from an online retailer. The data subject wants to pay by credit card and for the products to be delivered to their home address. In order to fulfil the contract, the retailer must process the data subject's credit card information and billing address for payment purposes and the data subject's home address for delivery. Thus, Article 6(1)(b) is applicable as a legal basis for these processing activities.

However, if the customer has opted for shipment to a pick-up point, the processing of the data subject's home address is no longer necessary for the performance of the purchase contract. Any processing of the data subject's address in this context will require a different legal basis than Article 6(1)(b).

示例1

當事人向線上零售商購買物品。當事人希望以信用卡付款，並將產品運送至其住家地址。為履行該契約，零售商必須為付款目的運用當事人的信用卡資訊與帳單地址、為運送目的運用當事人的住家地址。因此，第6條第1項第b款可作為此等運用活動的法律依據。

然而，若消費者選擇運送至取貨點，則運用當事人之住家地址即不再為履行該買賣契約所必要。此時，對當事人地址之運用活動將需要第6條第1項第b款以外的其他法律依據。

Example 2

The same online retailer wishes to build profiles of the user's tastes and lifestyle choices based on their visits to the website. Completion of the purchase contract is not dependent upon building such profiles. Even if profiling is specifically mentioned in the contract, this fact alone does not make it 'necessary' for the performance of the contract. If the online retailer wants to carry out such profiling, it needs to rely on a different legal basis.

示例2

同一線上零售商希望根據使用者對網站的瀏覽狀況，剖析其品味與

生活方式。完成買賣契約並不需要此等剖析。即使契約中明文涉及剖析作業，僅憑這一事實並不使之成為履行該契約所「必要」。該線上零售商如希望實施此等剖析，需要援用其他法律依據。

36. Within the boundaries of contractual law, and if applicable, consumer law, controllers are free to design their business, services and contracts. In some cases, a controller may wish to bundle several separate services or elements of a service with different fundamental purposes, features or rationale into one contract. This may create a ‘take it or leave it’ situation for data subjects who may only be interested in one of the services.

在契約法以及消費者保護法（如適用）之範圍內，控管者得自由設計其業務、服務與契約。某些情形下，控管者可能希望在同一契約中，納入根本目的、特徵或意旨不同的數種獨立服務或服務要素。對於僅對其中一項服務感興趣的當事人而言，這可能造成「全盤接受或全盤拒絕」的局面。

37. As a matter of data protection law, controllers need to take into account that the processing activities foreseen must have an appropriate legal basis. Where the contract consists of several separate services or elements of a service that can in fact reasonably be performed independently of one another, the question arises to which extent Article 6(1)(b) can serve as a legal basis. The applicability of Article 6(1)(b) should be assessed in the context of each of those services *separately*, looking at what is objectively necessary to perform each of the individual services which the data subject has actively requested or signed up for. This assessment may reveal that certain processing activities are not necessary for the individual services requested by the data subject, but rather necessary for the controller’s wider business model. In that case, Article 6(1)(b) will not be a legal basis for those activities. However, other legal bases may be available for that processing, such as Article 6(1)(a) or (f), provided that the relevant criteria are met. Therefore, the assessment of the applicability of Article 6(1)(b) does not affect the legality of the contract or the bundling of services as such.

就資料保護法而言，控管者須考量所預期的運用活動必須具有適當

的法律依據。若契約包含數種不同服務或服務要素，且其事實上可彼此獨立履行，則將產生第6條第1項第b款在何種程度上可作為法律依據之問題。第6條第1項第b款之可適用性應針對各項服務進行個別評估，檢視當事人所請求或同意的各項服務之履行以何者為客觀必要。此一評估可能揭示特定運用活動並非當事人所請求的個別服務所必要，而是為控管者更廣泛的商業模式所必要。此時，第6條第1項第b款並非此等運用活動之法律依據。然而，在滿足相應條件的前提下，可能適用其他法律依據，如第6條第1項第a款或第f款。因此，第6條第1項第b款之可適用性評估並不影響契約或服務捆綁行為本身之合法性。

38. As WP29 has previously observed, the legal basis only applies to what is necessary for the *performance* of a contract.²³ As such, it does not automatically apply to all further actions triggered by non-compliance or to all other incidents in the execution of a contract. However, certain actions can be reasonably foreseen and necessary within a normal contractual relationship, such as sending formal reminders about outstanding payments or correcting errors or delays in the performance of the contract. Article 6(1)(b) may cover processing of personal data which is necessary in relation to such actions.

如第29條工作小組之前所述，本法律依據僅適用於為履行契約所必要²³。因此，其並不自動適用於契約不履行或契約實施過程中的其他事件所引發的一切後續行動。然而，可合理預見特定行為係為正常契約關係所必要，如針對拖欠款項發出正式提醒，或糾正契約履行之錯誤或遲延。第6條第1項第b款可能涵蓋為此等行為所必要之個人資料運用活動。

Example 3

A company sells products online. A customer contacts the company because the colour of the product purchased is different from what was agreed upon. The processing of personal data of the customer for the

²³ Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217) page 17–18.

第29條工作小組「關於指令95/46/EC第7條之資料控管者正當利益概念之意見06/2014」(WP217)，頁17-18。

purpose of rectifying this issue can be based on Article 6(1)(b).

示例3

一家公司在網路上銷售產品。一名消費者因所購產品之顏色不符初始同意而聯絡該公司。為改正此問題而運用該消費者之個人資料，得以第6條第1項第b款為依據。

39. Contractual warranty may be part of performing a contract, and thus storing certain data for a specified retention time after exchange of goods/services/payment has been finalised for the purpose of warranties may be necessary for the performance of a contract.

契約擔保可能是履行契約之一部分，因此，在商品/服務/款項交換完成後，為保固目的而將某些資料保留特定期間，可能係為履行契約所必要。

2.6 Termination of contract

契約之終止

40. A controller needs to identify the appropriate legal basis for the envisaged processing operations before the processing commences. Where Article 6(1)(b) is the basis for some or all processing activities, the controller should anticipate what happens if that contract is terminated.²⁴

在開始運用前，控管者需為所預想的運用活動識別適當法律依據。若第6條第1項第b款係此等運用活動之全部或一部之依據，則控管者應預估契約終止後之狀況²⁴。

41. Where the processing of personal data is based on Article 6(1)(b) and the contract is terminated in full, then as a general rule, the processing of that data will no longer be necessary for the performance of that contract and thus the controller will need to stop processing. The data

²⁴ If a contract is subsequently invalidated, it will impact the lawfulness (as understood in Article 5(1)(a)) of continued processing. However, it does not automatically imply that the choice of Article 6(1)(b) as the legal basis was incorrect.

若契約後來被認定無效，將影響繼續運用（在第5條第1項第a款意義上）的合法性。然而，這並不必然表示選擇以第6條第1項第b款為法律依據是錯誤的。

subject might have provided their personal data in the context of a contractual relationship trusting that the data would only be processed as a necessary part of that relationship. Hence, it is generally unfair to swap to a new legal basis when the original basis ceases to exist.

若個人資料係基於第6條第1項第b款而運用，且契約已完全終止，一般而言，資料運用不再為履行該契約所必要，控管者因此須停止運用。當事人可能在契約關係存續期間，提供其個人資料，信任該等資料之運用將以契約關係之必要部分為限。因此，在原有依據不復存在後，轉換至新的法律依據，通常有失公平。

42. When a contract is terminated, this may entail some administration, such as returning goods or payment. The associated processing may be based on Article 6(1)(b).

契約終止後，可能需進行一些管理，如返還商品或款項。相關運用得以第6條第1項第b款為依據。

43. Article 17(1)(a) provides that personal data shall be erased when they are no longer necessary in relation to the purposes for which they were collected. Nonetheless, this does not apply if processing is necessary for certain specific purposes, including compliance with a legal obligation pursuant to Article 17(3)(b), or the establishment, exercise or defence of legal claims, pursuant to Article 17(3)(e). In practice, if controllers see a general need to keep records for legal purposes, they need to identify a legal basis for this at the outset of processing, and they need to communicate clearly from the start for how long they plan to retain records for these legal purposes after the termination of a contract. If they do so, they do not need to delete the data upon the termination of the contract.

第17條第1項第a款規定，個人資料對蒐集之目的不再必要者，應予以刪除。然而，本款並不適用於係為某些特定目的所必要之運用，包括依第17條第3項第b款遵守法定義務，或依第17條第3項第e款建立、行使或防禦法律上之請求。實際上，若控管者為法律目的而有保存紀錄的需求，其在運用開始時即須識別法律依據，且需自始便明確溝通其在契約終止後為法律目的保存紀錄之預定期間。若依此行事，其無需在契約終止後刪除資料。

44. In any case, it may be that several processing operations with separate purposes and legal bases were identified at the outset of processing. As long as those other processing operations remain lawful and the controller communicated clearly about those operations at the commencement of processing in line with the transparency obligations of the GDPR, it will still be possible to process personal data about the data subject for those separate purposes after the contract has been terminated.

無論如何，運用開始時，可能已識別出數個目的與法律依據各不相同的運用活動。只要該等其他運用活動仍屬合法，且控管者在運用開始時即已依GDPR之透明化義務明確溝通這些活動，則在契約終止後，仍可為其他獨立目的而運用當事人之個人資料。

Example 4

An online service provides a subscription service that can be cancelled at any time. When a contract for the service is concluded, the controller provides information to the data subject on the processing of personal data.

The controller explains, *inter alia*, that as long as the contract is in place, it will process data about the use of the service to issue invoices. The applicable legal basis is Article 6(1)(b) as the processing for invoicing purposes can be considered to be objectively necessary for the performance of the contract. However, when the contract is terminated and assuming there are no pending, relevant legal claims or legal requirements to retain the data, the usage history will be deleted.

Furthermore, the controller informs data subjects that it has a legal obligation in national law to retain certain personal data for accounting purposes for a specified number of years. The appropriate legal basis is Article 6(1)(c), and retention will take place even if the contract is terminated.

示例4

一項線上服務提供可隨時取消之訂閱服務。該服務契約訂立後，控管者向當事人提供運用個人資料之資訊。

控管者解釋，(尤其包括)只要契約存續，其將運用服務使用狀況之資料，以開立發票。可適用之法律依據為第6條第1項第b款，因為開立發票目的可視為履行契約所客觀必要。然而，契約終止後，設若無其他尚未解決之相關法律請求或保存該資料之法律要求，則該使用歷史應予以刪除。

此外，控管者告知當事人依據國內法，其負有為會計目的將特定個人資料保存特定年限之法定義務。可適用之法律依據為第6條第1項第c款，且契約終止後，將繼續保留資料。

2.7 Necessary for taking steps prior to entering into a contract 為締約前採取步驟所必要

45. The second option of Article 6(1)(b) applies where *processing is necessary in order to take steps at the request of the data subject prior to entering into a contract*. This provision reflects the fact that preliminary processing of personal data may be necessary before entering into a contract in order to facilitate the actual entering into that contract.

若運用係締約前應當事人之要求採取步驟所必要，則適用第6條第1項第b款的第二個選項。本條反映出在締約前，為協助實際締約所必要，可能需要初步運用個人資料之事實。

46. At the time of processing, it may not be clear whether a contract will actually be entered into. The second option of Article 6(1)(b) may nonetheless apply as long as the data subject makes the request in the context of *potentially* entering into a contract and the processing in question is necessary to take the steps requested. In line with this, where a data subject contacts the controller to enquire about the details of the controller's service offerings, the processing of the data subject's personal data for the purpose of responding to the enquiry can be based on Article 6(1)(b).

運用時，可能尚不明確能否實際締約。然而，只要當事人在可能締約之情況下提出請求，且運用係為採取請求步驟所必要，即可能適用第6條第1項第b款的第二個選項。因此，若當事人聯絡控管者，詢問控管者服務之細節，為回應該詢問而運用當事人之個人資料，得以第6條第1項第b款為依據。

47. In any case, this provision would not cover unsolicited marketing or other processing which is carried out solely on the initiative of the data controller, or at the request of a third party.

無論如何，本規定不涵蓋主動提供之行銷，或僅由資料控管者主動實施或應第三方請求而實施的其他運用。

Example 5

A data subject provides their postal code to see if a particular service provider operates in their area. This can be regarded as processing necessary to take steps at the request of the data subject prior to entering into a contract pursuant to Article 6(1)(b).

示例5

當事人提供其郵遞區號，以查看某一服務是否在其所在地提供。這可視為第6條第1項第b款之締約前應當事人要求採取步驟所必要之運用。

Example 6

In some cases, financial institutions have a duty to identify their customers pursuant to national laws. In line with this, before entering into a contract with data subjects, a bank requests to see their identity documents.

In this case, the identification is necessary for a legal obligation on behalf of the bank rather than to take steps at the data subject's request. Therefore, the appropriate legal basis is not Article 6(1)(b), but Article 6(1)(c).

示例6

某些情形下，金融機構依其國內法，有義務識別其客戶。因此，在與當事人締約前，銀行可能要求檢視其身分文件。

此時，身分識別乃為銀行負有之法定義務所必要，而非應當事人要求採取步驟。因此，適當之法律依據並非第6條第1項第b款，而是第6條第1項第c款。

3 PART 3 – APPLICABILITY OF ARTICLE 6(1)(B) IN SPECIFIC SITUATIONS

第3部分—特定情境中第6條第1項第b款之可適用性

3.1 Processing for ‘service improvement’²⁵

為「改進服務」而運用²⁵

48. Online services often collect detailed information on how users engage with their service. In most cases, collection of organisational metrics relating to a service or details of user engagement, cannot be regarded as necessary for the provision of the service as the service could be delivered in the absence of processing such personal data. Nevertheless, a service provider may be able to rely on alternative lawful bases for this processing, such as legitimate interest or consent.

線上服務通常蒐集使用者參與其服務之詳細資訊。大多數情況下，蒐集某項服務之組織數據（organisational metric）或使用使用者參與之詳細資訊，不得視為提供服務所必要，因為即使不運用此等個人資料，亦可提供服務。然而，對於此等運用，服務提供者可能援用其他合法依據，如正當利益或同意。

49. The EDPB does not consider that Article 6(1)(b) would generally be an appropriate lawful basis for processing for the purposes of improving a service or developing new functions within an existing service. In most cases, a user enters into a contract to avail of an existing service. While the possibility of improvements and modifications to a service may routinely be included in contractual terms, such processing usually cannot be regarded as being objectively necessary for the performance of the contract with the user.

對於為改進服務或開發現有服務新功能目的之運用，EDPB並不認為第6條第1項第b款一般可作為適當合法依據。大多數情況下，使用者締約係為了利用現有服務。雖然契約條款往往包括服務之改進與修

²⁵ Online services may also need to take into account Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.05.2019, p. 1), which will apply as from 1 January 2022.

線上服務可能還需考慮歐洲議會與歐盟理事會於2019年5月20日通過之「關於數位內容和數位服務供應契約相關面向之指令(EU) 2019/770」（OJ L 136, 22.05.2019, p. 1），該指令將於2022年1月1日施行。

改，此等運用通常不得視為係為履行與當事人間之契約所客觀必要。

3.2 Processing for ‘fraud prevention’

為「防範詐欺」而運用

50. As WP29 has previously noted,²⁶ processing for fraud prevention purposes may involve monitoring and profiling customers. In the view of the EDPB, such processing is likely to go beyond what is objectively necessary for the performance of a contract with a data subject. However, the processing of personal data strictly necessary for the purposes of preventing fraud may constitute a legitimate interest of the data controller²⁷ and could thus be considered lawful, if the specific requirements of Article 6(1)(f)(legitimate interests) are met by the data controller. In addition Article 6(1)(c) (legal obligation) could also provide a lawful basis for such processing of data.

如第29條工作小組之前所指出²⁶，為防範詐欺目的運用資料可能涉及對消費者的監控與剖析。EDPB認為，此等運用很可能超出為履行與當事人間之契約所客觀必要之範圍。然而，出於防範詐欺目的之絕對必要而運用個人資料，可能構成資料控管者的正當利益²⁷，因此在資料控管者滿足第6條第1項第f款（正當利益）之具體要求時，可能被視為合法。此外，第6條第1項第c款（法定義務）亦可能作為此等資料運用之合法依據。

3.3 Processing for online behavioural advertising

為線上行為廣告而運用

51. Online behavioural advertising, and associated tracking and profiling of data subjects, is often used to finance online services. WP29 has previously stated its view on such processing, stating:

線上行為廣告及其相關之當事人追蹤與剖析，是線上服務獲利之常見方法。第29條工作小組之前曾對此等運用表明觀點，認為：

[contractual necessity] is not a suitable legal ground for building a profile

²⁶ Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), page 17.

第29條工作小組「關於指令95/46/EC第7條之資料控管者正當利益概念之意見06/2014」（WP217），頁17。

²⁷ See Recital 47, sixth sentence.

見前言第47點，第6句。

*of the user's tastes and lifestyle choices based on his clickstream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example.*²⁸

[契約必要性] 對於「根據使用者在網站上的點擊流與購買品項，對其品味及生活方式建立剖析」，並非適當的法律依據。這是由於資料控管者之契約並非為了實施剖析，而是基於例如提供特定商品和服務之目的²⁸。

52. As a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services. Normally, it would be hard to argue that the contract had not been performed because there were no behavioural ads. This is all the more supported by the fact that data subjects have the absolute right under Article 21 to object to processing of their data for direct marketing purposes.

一般而言，為行為廣告而運用個人資料並非履行線上服務契約所必要。通常難以主張未履行契約是因為缺乏行為廣告。更能佐證這一點的事實是，當事人依第21條對為行銷目的的資料運用活動享有絕對拒絕權。

53. Further to this, Article 6(1)(b) cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service. Although such processing may support the delivery of a service, this in itself is not sufficient to establish that it is necessary for the performance of the contract at issue. The controller would need to consider the factors outlined in paragraph 33.

更進一步而言，無法僅因線上行為廣告間接資助服務之提供，而認為第6條第1項第b款為此等廣告提供合法依據。雖然此等運用可能支援服務之提供，這本身並不足以確立此係履行相應契約所必要。控管者需考量第33段所列要素。

54. Considering that data protection is a fundamental right guaranteed by

²⁸ Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), page 17.

第29條工作小組「關於指令95/46/EC第7條之資料控管者正當利益概念之意見06/2014」(WP217)，頁17。

Article 8 of the Charter of Fundamental Rights, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over information relating to them, personal data cannot be considered as a tradeable commodity. Even if the data subject can agree to the processing of personal data,²⁹ they cannot trade away their fundamental rights through this agreement.³⁰

由於資料保護乃「基本權利憲章」第8條所保障之基本權利，考量GDPR之主要目的之一係賦予當事人對其相關資訊之控制權，個人資料不得被視作可供交易之財貨。當事人雖可同意個人資料之運用²⁹，卻無法透過契約出售其基本權利³⁰。

55. The EDPB also notes that, in line with ePrivacy requirements and the existing WP29 opinion on behavioural advertising,³¹ and Working Document 02/2013 providing guidance on obtaining consent for cookies,³² controllers must obtain data subjects' prior consent to place the cookies necessary to engage in behavioural advertising.

EDPB還指出，依電子隱私要求、現行第29條工作小組關於行為廣告之意見³¹，以及為獲取cookie同意提供指導之工作文件02/2013³²，控管者在為行為廣告而置入所需的cookies時，必須獲得當事人的事前同意。

56. The EDPB also notes that tracking and profiling of users may be carried out for the purpose of identifying groups of individuals with similar

²⁹ See Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

見歐洲議會與歐盟理事會於2019年5月20日通過之「關於數位內容和數位服務供應契約相關面向之指令(EU) 2019/770」。

³⁰ Besides the fact that the use of personal data is regulated by the GDPR, there are additional reasons why processing of personal data is conceptually different from monetary payments. For example, money is countable, meaning that prices can be compared in a competitive market, and monetary payments can normally only be made with the data subject's involvement. Furthermore, personal data can be exploited by several services at the same time. Once control over one's personal data has been lost, that control may not necessarily be regained.

除使用個人資料受GDPR規範之事實外，運用個人資料與金錢給付還因其他原因而存在概念性區別。例如，金錢是可計算的，意即可在競爭市場中比較價格，且金錢給付通常非經當事人參與無法完成。此外，個人資料可供數項服務同時利用。一旦喪失對個人資料之控制，未必能夠重掌控制。

³¹ Article 29 Working Party Opinion 2/2010 on online behavioural advertising (WP171).

第29條工作小組「關於線上行為廣告之意見2/2010」（WP171）。

³² Article 29 Working Party Working Document 02/2013 providing guidance on obtaining consent for cookies (WP208).

第29條工作小組「為獲取cookie同意提供指導之工作文件02/2013」（WP208）。

characteristics, to enable targeting advertising to similar audiences. Such processing cannot be carried out on the basis of Article 6(1)(b), as it cannot be said to be objectively necessary for the performance of the contract with the user to track and compare users' characteristics and behaviour for purposes which relate to advertising to other individuals.³³ EDPB還指出，使用者追蹤和剖析可能係為了識別具有類似特徵的個人群體，以便向類似對象投放定向廣告。實施此等運用不得以第6條第1項第b款為依據，原因在於，為了向他人投放廣告之目的而追蹤和比較多數使用者的特徵與行為，無法解釋為係履行與該使用者間契約所客觀必要³³。

3.4 Processing for personalisation of content³⁴ 為個人化內容而運用³⁴

57. The EDPB acknowledges that personalisation of content may (but does not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract with the service user in some cases. Whether such processing can be regarded as an intrinsic aspect of an online service, will depend on the nature of the service provided, the expectations of the average data subject in light not only of the terms of service but also the way the service is promoted to users, and whether the service can be provided without personalisation. Where personalisation of content is not objectively necessary for the purpose of the underlying contract, for example where personalised content delivery is intended to increase user engagement with a service but is not an integral part of using the service, data controllers should consider an alternative lawful basis where applicable.

³³ See also Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), endorsed by the EDPB, page 13.

另見第29條工作小組「關於第2016/679號規則（GDPR）中的自動化個人決策和剖析之指引」（WP251rev.01），EDPB採認，頁13。

³⁴ Online services may also need to take into account Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.05.2019, p. 1), which will apply as from 1 January 2022.

線上服務可能還需考慮歐洲議會與歐盟理事會於2019年5月20日通過之「關於數位內容和數位服務供應契約相關面向之指令(EU) 2019/770」（OJ L 136, 22.05.2019, p. 1），該指令將於2022年1月1日施行。

EDPB承認，個人化內容可能（但並非總是）構成特定線上服務一項被期待的本質要素，因此可能在某些情形下被視為履行與服務使用者間契約所必要。此等運用能否被視為某一線上服務的本質面向之一，取決於所提供服務之性質、一般當事人的期待（不僅考量服務條款，還考量服務如何推銷給使用者），以及該服務能否不經個人化而提供。若個人化內容並非該契約目的所客觀必要，如個人化內容之目的係為了增進使用者對服務之參與，而非利用該服務所不可或缺之一部分，資料控管者應考量其他可適用之合法依據。

Example 7

An online hotel search engine monitors past bookings of users in order to create a profile of their typical expenditure. This profile is subsequently used to recommend particular hotels to the user when returning search results. In this case, profiling of user's past behaviour and financial data would not be objectively necessary for the performance of a contract, i.e. the provision of hospitality services based on particular search criteria provided by the user. Therefore, Article 6(1)(b) would not be applicable to this processing activity.

示例7

一家線上旅館搜尋引擎監控使用者的訂房紀錄，以剖析其通常消費。此等剖析結果隨後被用於在搜尋結果中向使用者推薦特定旅館。這種情形下，剖析使用者的過往行為與財務資料並非履行契約所客觀必要，也就是該契約係依使用者提供之搜尋條件提供餐旅服務。因此，第6條第1項第b款不適用於此等運用行為。

Example 8

An online marketplace allows potential buyers to browse for and purchase products. The marketplace wishes to display personalised product suggestions based on which listings the potential buyers have previously viewed on the platform in order to increase interactivity. This personalisation it is not objectively necessary to provide the marketplace service. Thus, such processing of personal data cannot rely on Article 6(1)(b) as a legal basis.

示例8

一家線上購物平台允許潛在買家瀏覽和購買產品。該平台希望依據潛在買家在該平台上已瀏覽過的商品，提供個人化的產品建議，以便提升互動性。這種個人化非為提供購物平台服務所客觀必要。因此，個人資料之此等運用不得以第6條第1項第b款為法律依據。

Guidelines



Guidelines 3/2019 on processing of personal data through video devices

關於以影像裝置運用個人資料之指引3/2019

Version 2.0

版本2.0

Adopted on 10 July 2019

2019年7月10日通過

Version history

版本更新歷程

Version 2.1 版本 2.1	26 February 2020 2020年2月26日	Amending material mistake 修正文字錯誤
Version 2.0 版本 2.0	29 January 2020 2020年1月29日	Adoption of the Guidelines after public consultation 公眾諮詢後通過本指引
Version 1.0 版本 1.0	10 July 2019 2019年7月10日	Adoption of the Guidelines for public consultation 通過本指引供公眾諮詢

Table of contents

目錄

1	Introduction 導言	6
2	Scope of application 適用範圍	9
2.1	Personal Data 個人資料	9
2.2	Application of the Law Enforcement Directive, LED (EU2016/680) 執法指令 (LED) (EU2016/680) 之適用	10
2.3	Household exemption 家庭活動例外	11
3	Lawfulness of processing 運用之合法性	14
3.1	Legitimate interest, Article 6 (1) (f) 正當利益，第6條第1項第f款	15
3.1.1	Existence of legitimate interests 存在正當利益	15
3.1.2	Necessity of processing 運用之必要性	17
3.1.3	Balancing of interests 利益衡平	20
3.2	Necessity to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, Article 6 (1) (e) 為執行符合公共利益之職務或行使公權力所必要，第6條第1 項第e款	25
3.3	Consent, Article 6 (1) (a) 同意，第6條第1項第a款	26
4	Disclosure of video footage to third parties 向第三方揭露影片	28
4.1	Disclosure of video footage to third parties in general 向第三方揭露影片概述	28
4.2	Disclosure of video footage to law enforcement agencies 向執法機關揭露影片	29
5	Processing of special categories of data 運用特種個資	32
5.1	General considerations when processing biometric data 運用生物特徵資料之一般考量	34

5.2	Suggested measures to minimize the risks when processing biometric data	
	運用生物特徵資料時將風險降到最小之建議措施.....	42
6	Rights of the data subject 當事人的權利	45
6.1	Right to access 近用權	45
6.2	Right to erasure and right to object 刪除權和拒絕權	48
6.2.1	Right to erasure (Right to be forgotten)	
	刪除權（被遺忘權）	48
6.2.2	Right to object 拒絕權	51
7	Transparency and information obligations	
	透明化和資訊提供義務.....	53
7.1	First layer information (warning sign)	
	第一層資訊（警示標誌）	54
7.1.1	Positioning of the warning sign 警示標誌之放置方式	54
7.1.2	Content of the first layer 第一層內容.....	55
7.2	Second layer information 第二層資訊	57
8	Storage periods and obligation to erasure	
	儲存期間和刪除義務	59
9	Technical and organisational measures	
	技術性和組織性措施	61
9.1	Overview of video surveillance system	
	影像監控系統概述	61
9.2	Data protection by design and by default	
	資料保護之設計和預設	64
9.3	Concrete examples of relevant measures	
	相關措施的具體示例.....	65
9.3.1	Organisational measures 組織性措施	67
9.3.2	Technical measures 技術性措施.....	68
10	Data protection impact assessment 個資保護影響評估.....	71

The European Data Protection Board

Having regard to Article 70 (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

歐盟個人資料保護委員會

依據歐洲議會與歐盟理事會於2016年4月27日通過之「關於運用*個人資料時對自然人之保護與確保此等資料之自由流通，以及廢除指令95/46/EC的歐盟規則2016/679/EU」（下稱GDPR）第70條第1項第e款；

依據歐洲經濟區聯合委員會於2018年7月6日第154/2018號決定修改之歐洲經濟區（EEA）協議，尤其是附件11及其議定書37¹；

依據「歐盟個人資料保護委員會議事規則」第12條和第22條；

通過以下指引：

* 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」。

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

本意見所稱之「會員國」應理解為「EEA會員國」。

1 INTRODUCTION

導言

1. The intensive use of video devices has an impact on citizen's behaviour. Significant implementation of such tools in many spheres of the individuals' life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed. Data protection implications are massive.

影像裝置的密集使用影響了公民之行為。此等工具在個人生活之諸多領域大量裝設，將使人需要防範別人探知其可能被視為異常之行為，從而給個人造成額外壓力。事實上，這些技術可能限制匿名行動和匿名使用服務之可能性，且會普遍限制保持不被注意狀態之可能性。這對於資料保護有深遠影響。

2. While individuals might be comfortable with video surveillance set up for a certain security purpose for example, guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.). In addition, many tools are now implemented to exploit the images captured and turn traditional cameras into smart cameras. The amount of data generated by the video, combined with these tools and techniques increase the risks of secondary use (whether related or not to the purpose originally assigned to the system) or even the risks of misuse. The general principles in GDPR (Article 5), should always be carefully considered when dealing with video surveillance.

雖然個人或許能夠接受錄影監控，例如為某些安全目的所裝設，仍必須採取保障措施，避免不當用於完全不同且（對於當事人而言）意料之外之目的（例如行銷目的、監控員工表現等）。此外，當前所裝設的諸多工具，係為利用所拍攝的畫面，並將傳統相機轉化為智慧相機。影像所生成之諸多資料，結合這些工具和技術，使得次級使用（secondary usage）（無論與系統設置之原始目的是否相關）、乃至不當使用之風險升高。處理影像監控議題時，應始終仔細考量GDPR之一般原則（第5條）。

3. Video surveillance systems in many ways change the way professionals

from the private and public sector interact in private or public places for the purpose of enhancing security, obtaining audience analysis, delivering personalized advertising, etc. Video surveillance has become high performing through the growing implementation of intelligent video analysis. These techniques can be more intrusive (e.g. complex biometric technologies) or less intrusive (e.g. simple counting algorithms). Remaining anonymous and preserving one's privacy is in general increasingly difficult. The data protection issues raised in each situation may differ, so will the legal analysis when using one or the other of these technologies.

影像監控系統在諸多方面改變了公私部門的專業人員為增進安全、獲取對象分析、投放個人化廣告等目的，在公私場所之互動。智慧影像分析逐漸普及，影像監控的性能也隨之提高。這些技術的干預性可能較高（例如複雜生物辨識技術），也可能較低（例如簡單計數演算法）。整體觀之，維持匿名和保護個人隱私越來越困難。各種情況下所涉及之資料保護議題可能不同，因此使用這些不同技術時的法律分析也存在差異。

4. In addition to privacy issues, there are also risks related to possible malfunctions of these devices and the biases they may induce. Researchers report that software used for facial identification, recognition, or analysis performs differently based on the age, gender, and ethnicity of the person it's identifying. Algorithms would perform based on different demographics, thus, bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided.

除隱私議題外，還可能存在裝置功能異常和引發偏見之風險。研究者發現，用於臉部識別、辨識或分析之軟體，其表現因被辨識者的年齡、性別和種族不同而有差異。演算法之表現依其分析之對象不同而有差異，因此，臉部辨識偏見可能加劇社會歧視。正是因此，對於影像監控衍生之生物特徵資料運用，資料控管者必須確保定期評估其相關性與保障措施充足性。

5. Video surveillance is not by default a necessity when there are other

means to achieve the underlying purpose. Otherwise we risk a change in cultural norms leading to the acceptance of lack of privacy as the general outset.

存在實現基本目的之其他方法時，影像監控未必是預設方案。否則，我們將面臨文化規範轉變，導致對缺乏隱私普遍接受之風險。

6. These guidelines aim at giving guidance on how to apply the GDPR in relation to processing personal data through video devices. The examples are not exhaustive, the general reasoning can be applied to all potential areas of use.

本指引目的係對GDPR如何適用於以影像裝置運用個人資料提供指導。相關示例並非完全列舉，其一般論理可適用於一切潛在之使用領域。

2 SCOPE OF APPLICATION²

適用範圍²

2.1 Personal Data

個人資料

7. Systematic automated monitoring of a specific space by optical or audio-visual means, mostly for property protection purposes, or to protect individual's life and health, has become a significant phenomenon of our days. This activity brings about collection and retention of pictorial or audio-visual information on all persons entering the monitored space that are identifiable on basis of their looks or other specific elements. Identity of these persons may be established on grounds of these details. It also enables further processing of personal data as to the persons' presence and behaviour in the given space. The potential risk of misuse of these data grows in relation to the dimension of the monitored space as well as to the number of persons frequenting the space. This fact is reflected by the General Data Protection Regulation in the Article 35 (3) (c) which requires the carrying out of a data protection impact assessment in case of a systematic monitoring of a publicly accessible area on a large scale, as well as in Article 37 (1) (b) which requires processors to designate a data protection officer, if the processing operation by its nature entails regular and systematic monitoring of data subjects.

主要為保護財產目的、或為保護個人生命和健康，以光學或影音手段系統性、自動化地監控特定空間，已成為日常生活中的重要現象。此一活動蒐集和保留進入該受監控空間的一切人員的圖像或影音資訊，且相關人員可基於其外表或其他特定要素而被識別。基於這些詳細資訊，可能確定這些人員之身分。這也使得相關人員在特定空間出現及其行為的個人資料可被進階運用。受監控空間的面積越大、經常出入該空間的人數越多，不當使用這些資料之風險也越高。GDPR第35條第3項第c款反映這一事實，要求對於公眾開放區域進行大規模、系統性之監控時，須辦理個資保護影響評估；第37條第1項

² The EDPB notes that where the GDPR so allows, specific requirements in national legislation might apply.

EDPB注意到，在GDPR許可的情況下，可能適用國家立法中的特定要求。

第b款也反應這一事實，要求受託運用者在運用作業本質需要經常性、系統性監控當事人時，指派個資保護長。

8. However, the Regulation does not apply to processing of data that has no reference to a person, e.g. if an individual cannot be identified, directly or indirectly.

然而，「規則」並不適用於與個人無關的資料運用活動，例如無法直接或間接識別個人之情況。

9.

Example: The GDPR is not applicable for fake cameras (i.e. any camera that is not functioning as a camera and thereby is not processing any personal data). However, in some Member States it might be subject to other legislation.

示例：GDPR並不適用於假的相機（亦即，無法發揮功能且因此不運用任何個人資料的相機）。然而，這在某些會員國可能受其他法律規範。

Example: Recordings from a high altitude only fall under the scope of the GDPR if under the circumstances the data processed can be related to a specific person.

示例：高空拍攝只有在其運用的資料關聯到特定個人時，方落入GDPR之適用範圍。

Example: A video camera is integrated in a car for providing parking assistance. If the camera is constructed or adjusted in such a way that it does not collect any information relating to a natural person (such as licence plates or information which could identify passers-by) the GDPR does not apply.

示例：汽車上裝設錄影鏡頭，以協助停車。若依該相機的裝設或調整方式，並不蒐集與自然人相關之任何資訊（例如車牌或可識別路人之資訊），則不適用GDPR。

2.2 Application of the Law Enforcement Directive, LED (EU2016/680) 執法指令（LED）（EU2016/680）之適用

10. Notably processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of

criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, falls under the directive EU2016/680.

值得注意的是，權責機關為預防、調查、偵查或起訴犯罪或執行刑罰（包括因應和防範公共安全威脅）而運用個人資料之行為，適用指令EU2016/680。

2.3 Household exemption

家庭活動例外

11. Pursuant to Article 2 (2) (c), the processing of personal data by a natural person in the course of a purely personal or household activity, which can also include online activity, is out of the scope of the GDPR.³

依第2條第2項第c款，自然人在單純個人或家庭活動過程中運用個人資料之行為(有可能包含線上活動)，在GDPR的適用範圍外³。

12. This provision – the so-called household exemption – in the context of video surveillance must be narrowly construed. Hence, as considered by the European Court of Justice, the so called “household exemption” must *“be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people”*.⁴ Furthermore, if a video surveillance system, to the extent it involves the constant recording and storage of personal data and covers, *“even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely ‘personal or household’ activity for the purposes of the second indent of Article 3(2) of Directive 95/46”*⁵.

在影像監控方面，本條——即所謂的家庭活動例外——須作狹義解釋。因此，正如歐洲法院之見解，所謂的「家庭活動例外」必須「解釋為僅與個人之私人或家庭生活過程中實施之活動相關，若在網路上公開資料、使之可為不特定多數人存取，此等個人資料運用活動顯

³ See also Recital 18.

另見前言第18點。

然非屬此類」⁴。此外，若影像監控系統經常性地錄製與儲存個人資料，且「（即使僅部分地）包含公共空間，並因此脫離個人運用資料之私人背景，則其不得被視為指令95/46第3條第2項第二點所規定的之單純『個人或家庭』活動」⁵。

13. What regards video devices operated inside a private person's premises, it may fall under the household exemption. It will depend on several factors, which all have to be considered in order to reach a conclusion. Besides the above mentioned elements identified by ECJ rulings, the user of video surveillance at home needs to look at whether he has some kind of personal relationship with the data subject, whether the scale or frequency of the surveillance suggests some kind of professional activity on his side, and of the surveillance's potential adverse impact on the data subjects. The presence of any single one of the aforementioned elements does not necessarily suggest that the processing is outside the scope of the household exemption, an overall assessment is needed for that determination.

至於在個人之私人處所內部運作之影像裝置，則可能落入家庭活動例外範圍內。這取決於數項要素，須全部予以考慮後方可得出結論。除上述歐洲法院（ECJ）確定的要素外，家庭影像監控的使用者需檢視其與當事人間是否存在某種私人關係，監控的規模與頻率是否意味著其在從事某種職業活動，以及監控對當事人的潛在不利影響。存在前述任何要素之一，並不必然意味著運用不屬於家庭活動例外，得出此一結論需進行整體評估。

14.

Example: A tourist is recording videos both through his mobile phone and through a camcorder to document his holidays. He shows the footage to friends and family but does not make it accessible for an indefinite number of people. This would fall under the household

⁴ European Court of Justice, Judgment in Case C-101/01, *Bodil Lindqvist case*, 6th November 2003, para 47.

歐洲法院，第C-101/01號案件（*Bodil Lindqvist*案）判決，2003年11月6日，第47段。

⁵ European Court of Justice, Judgment in Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11 December 2014, para. 33.

歐洲法院，第C-212/13號案件（*František Ryneš v Úřad pro ochranu osobních údajů*）判決，2014年12月11日，第33段。

exemption.

示例：一名遊客同時使用其手機和錄影機記錄其假期。他讓朋友和家人觀看該影片，但並未將其提供給不特定多數人。這將適用家庭活動例外。

Example: A downhill mountain biker wants to record her descent with an actioncam. She is riding in a remote area and only plans to use the recordings for her personal entertainment at home. This would fall under the household exemption even if to some extent personal data is processed.

示例：一名下坡山地車手想要以運動攝影機攝錄其下坡過程。她在偏遠地區騎行，且計劃將所錄影片僅用於在家私人欣賞。即使在某種程度上運用個人資料，這也屬於家庭活動例外。

Example: Somebody is monitoring and recording his own garden. The property is fenced and only the controller himself and his family are entering the garden on a regular basis. This would fall under the household exemption, provided that the video surveillance does not extend even partially to a public space or neighbouring property.

示例：某人對其自己的花園進行監控錄影。該花園裝有圍欄，且僅有控管者及其家人會經常進出。若該影像監控並不（即使部分地）延伸至公共空間或鄰近地產，亦屬於家庭活動例外。

3 LAWFULNESS OF PROCESSING

運用之合法性

15. Before use, the purposes of processing have to be specified in detail (Article 5 (1) (b)). Video surveillance can serve many purposes, e.g. supporting the protection of property and other assets, supporting the protection of life and physical integrity of individuals, collecting evidence for civil claims.⁶ These monitoring purposes should be documented in writing (Article 5 (2)) and need to be specified for every surveillance camera in use. Cameras that are used for the same purpose by a single controller can be documented together. Furthermore, data subjects must be informed of the purpose(s) of the processing in accordance with Article 13 (*see section 7, Transparency and information obligations*). Video surveillance based on the mere purpose of “safety” or “for your safety” is not sufficiently specific (Article 5 (1) (b)). It is furthermore contrary to the principle that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (*see Article 5 (1) (a)*).

在使用前，須特定運用之目的（第5條第1項第b款）。影像監控可用於諸多目的，例如支援財產和其他資產之保全、支援個人生命和人身安全之保護、為民事主張蒐集證據等⁶。應書面記錄這些監控目的（第5條第2項），且對所使用的每個監控攝影機均應特定其目的。同一控管者為同樣目的使用之多個攝影機得合併紀錄。此外，須依第13條（見第7節，透明化和資訊提供義務）向當事人告知運用之目的。僅以「安全」或「為你的安全」作為影像監控之目的，並不夠具體特定（第5條第1項第b款）。這還違反資料運用應以合法、公平合理且對當事人以透明之方式為之的原則（見第5條第1項第a款）。

16. In principle, every legal ground under Article 6 (1) can provide a legal basis for processing video surveillance data. For example, Article 6 (1) (c) applies where national law stipulates an obligation to carry out video surveillance.⁷ However in practice, the provisions most likely to be used are

原則上，第6條第1項規定的各款法律依據皆可作為運用影像監控資

⁶ Rules on collecting evidence for civil claims varies in Member States.
會員國關於民事主張的蒐證規則存在差異。

料之依據。例如，國內法規定實施影像監控之義務時，適用第6條第1項第c款⁷。但實務中，最可能使用的條款為：

- Article 6 (1) (f) (legitimate interest),
第6條第1項第f款（正當利益），
- Article 6 (1) (e) (necessity to perform a task carried out in the public interest or in the exercise of official authority).
第6條第1項第e款（為執行符合公共利益之職務或行使公權力所必要）。

In rather exceptional cases Article 6 (1) (a) (consent) might be used as a legal basis by the controller.

在相當例外的情形下，控管者可能以第6條第1項第a款（同意）為法律依據。

3.1 Legitimate interest, Article 6 (1) (f)

正當利益，第6條第1項第f款

17. The legal assessment of Article 6 (1) (f) should be based on the following criteria in compliance with Recital 47.

第6條第1項第f款之法律評估應依據前言第47點，基於下列標準實施。

3.1.1 Existence of legitimate interests

存在正當利益

18. Video surveillance is lawful if it is necessary in order to meet the purpose of a legitimate interest pursued by a controller or a third party, unless such interests are overridden by the data subject's interests or fundamental rights and freedoms (Article 6 (1) (f)). Legitimate interests pursued by a controller or a third party can be legal,⁸ economic or non-material interests.⁹ However, the controller should consider that if the data subject objects to the surveillance in accordance with Article 21 the controller can only proceed with the video surveillance of that data subject if it is a compelling legitimate interest which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

⁷ These guidelines do not analyse or go into details of national law that might differ between Member States.

本指引並不分析或深入討論國內法，各會員國的國內法可能不同。

若影像監控係為了滿足控管者或第三方所追求之正當利益目的所必要，則監控為合法，除非其利益被當事人之利益或基本權利與自由所超越（第6條第1項第f款）。控管者或第三方所追求之正當利益可能為法律上⁸、經濟上或非財物利益⁹。然而，控管者應考慮，若當事人依第21條拒絕監控，則控管者僅得在下列情形實施影像監控：存在超越當事人利益、權利和自由之必要正當利益，或為建立、行使或防禦法律上之請求。

19. Given a real and hazardous situation, the purpose to protect property against burglary, theft or vandalism can constitute a legitimate interest for video surveillance.

於存在真實危險之情形下，保護財產免受非法入室、竊盜、故意破壞之目的，得構成影像監控之正當利益。

20. The legitimate interest needs to be of real existence and has to be a present issue (i.e. it must not be fictional or speculative)¹⁰. A real-life situation of distress needs to be at hand – such as damages or serious incidents in the past – before starting the surveillance. In light of the principle of accountability, controllers would be well advised to document relevant incidents (date, manner, financial loss) and related criminal charges. Those documented incidents can be a strong evidence for the existence of a legitimate interest. The existence of a legitimate interest as well as the necessity of the monitoring should be reassessed in periodic intervals (e. g. once a year, depending on the circumstances). 正當利益需真實存在，且須為現存之問題（即不得為假想或猜測）¹⁰。在開始監控前，需現實存在迫切危難—例如損害或過去發生的嚴重事故。依課責性原則，建議控管者宜記錄相關事故（日期、方式、經濟損失）和相關刑事控告。所記錄的事故可作為存在正當利益的有力證據。應定期重新評估是否存在正當利益和監控必要性（例如根據情形每年一次）。

⁸ European Court of Justice, Judgment in Case C-13/16, *Rīgas satiksme case*, 4 may 2017.

歐洲法院，第C-13/16號案件（*Rīgas satiksme*案）判決，2017年5月4日。

⁹ see wp 217, Article 29 Working Party.

見wp217，第29條工作小組。

¹⁰ see wp 217, Article 29 Working Party, p. 24 seq. See also ECJ Case C-708/18 p.44

見wp217，第29條工作小組，第24頁以下。另見歐洲法院第C-708/18號案件，第44段（譯註：原文第44頁應為誤植）。

21.

Example: A shop owner wants to open a new shop and wants to install a video surveillance system to prevent vandalism. He can show, by presenting statistics, that there is a high expectation of vandalism in the near neighbourhood. Also, experience from neighbouring shops is useful. It is not necessary that a damage to the controller in question must have occurred. As long as damages in the neighbourhood suggest a danger or similar, and thus can be an indication of a legitimate interest. It is however not sufficient to present national or general crime statistic without analysing the area in question or the dangers for this specific shop.

示例：一名店主希望開設一間新店，且想要裝設影像監控系統以防範故意破壞行為。其可通過展示統計數據，論證其鄰近地區故意破壞行為的可能性很高。此外，附近商店的經驗也是有用的。該控管者並不一定已受損失。只要鄰近地區的損失已表明存在危險或類似事由，即可作為正當利益之表徵。然而，若僅提出全國性或一般性的犯罪統計數據，而未分析相關地區或該特定商店面臨的危險，則並不足夠。

22. Imminent danger situations may constitute a legitimate interest, such as banks or shops selling precious goods (e.g. jewellers), or areas that are known to be typical crime scenes for property offences (e. g. petrol stations).

迫切危險情形可構成正當利益，比如銀行或銷售貴重商品（例如珠寶）之商店，或公認的財產犯罪常見地點（例如加油站）。

23. The GDPR also clearly states that public authorities cannot rely their processing on the grounds of legitimate interest, as long as they are carrying out their tasks, Article 6 (1) sentence 2.

GDPR第6條第1項第2句還明確規定，公務機關在執行公務時，不得援用正當利益作為運用之依據。

3.1.2 Necessity of processing

運用之必要性

24. Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data

minimisation'), see Article 5 (1) (c). Before installing a video-surveillance system the controller should always critically examine if this measure is firstly suitable to attain the desired goal, and secondly adequate and necessary for its purposes. Video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means which are less intrusive to the fundamental rights and freedoms of the data subject.

個人資料應適當、相關且限於其運用目的所必要（「資料最小化」），見第5條第1項第c款。在裝設影像監控系統前，控管者首先應總是審慎檢視此一措施是否適合實現所預期目的，其次對其目的是否適當且必要。唯有對當事人之基本權利與自由干預性較低之其他措施無法合理實現運用之目的時，方得選擇影像監控措施。

25. Given the situation that a controller wants to prevent property related crimes, instead of installing a video surveillance system the controller could also take alternative security measures such as fencing the property, installing regular patrols of security personnel, using gatekeepers, providing better lighting, installing security locks, tamper-proof windows and doors or applying anti-graffiti coating or foils to walls. Those measures can be as effective as video surveillance systems against burglary, theft and vandalism. The controller has to assess on a case-by-case basis whether such measures can be a reasonable solution.

在防範財產犯罪的情境中，控管者可能不裝設影像監控系統，而是採取替代性安全措施，例如對財產架設圍欄、由保全人員定期巡視、設置門衛、提供更佳照明、安裝安全鎖和防盜門窗，或對牆壁使用防塗鴉塗層或貼膜。在防範非法入室、竊盜、故意破壞財物方面，這些措施與影像監控系統同樣有效。控管者必須對個案評估這些措施是否為合理解決方案。

26. Before operating a camera system, the controller is obliged to assess where and when video surveillance measures are strictly necessary. Usually a surveillance system operating at night-time as well as outside the regular working hours will meet the needs of the controller to prevent any dangers to his property.

在運作錄影系統前，控管者有義務評估影像監控系統在何時及何地有絕對必要性。通常，在夜間和正常工作時間外運作之監控系統將

滿足控管者防範財產損害危險之需求。

27. In general, the necessity to use video surveillance to protect the controllers' premises ends at the property boundaries¹¹ However, there are cases where the surveillance of the property is not sufficient for an effective protection. In some individual cases it might be necessary to exceed the video surveillance to the immediate surroundings of the premises. In this context, the controller should consider physical and technical means, for example blocking out or pixelating not relevant areas.

一般而言，使用影像監控保護控管者處所的必要性止於其財產的邊界¹¹。然而，某些情形下，對財產的監控並不足以提供有效保護。某些個別情形下，可能有必要將影像監控擴張到場所密切相鄰之範圍。此時，控管者應考慮實體（physical）與技術方法，例如遮蔽不相關區域或打馬賽克（pixelate）。

28.

Example: A bookshop wants to protect its premises against vandalism. In general, cameras should only be filming the premises itself because it is not necessary to watch neighbouring premises or public areas in the surrounding of the bookshop premises for that purpose.

示例：一家書店想要防範對其經營場所的故意破壞活動。一般而言，攝影機應僅攝錄該經營場所本身，因為此一目的不需要監控附近其他場所或該書店周邊的公共空間。

29. Questions concerning the processing's necessity also arise regarding the way evidence is preserved. In some cases it might be necessary to use black box solutions where the footage is automatically deleted after a certain storage period and only accessed in case of an incident. In other situations, it might not be necessary to record the video material at all but more appropriate to use real-time monitoring instead. The decision between black box solutions and real-time monitoring should also be based on the purpose pursued. If for example the purpose of video surveillance is the preservation of evidence, real-time methods are usually not suitable. Sometimes real-time monitoring may also be more

¹¹ This might also be subject to national legislation in some Member States.
在某些會員國，這可能也受國內立法規範。

intrusive than storing and automatically deleting material after a limited timeframe (e. g. if someone is constantly viewing the monitor it might be more intrusive than if there is no monitor at all and material is directly stored in a black box). The data minimisation principle must be regarded in this context (Article 5 (1) (c)). It should also be kept in mind that it might be possible that the controller could use security personnel instead of video surveillance that are able to react and intervene immediately.

證據的保存方式也可能引發運用的必要性問題。某些情形下，可能有必要運用黑箱（black box）方案，即影片於保存一定期間後自動刪除，且僅於發生事故時才被存取。其他情形下，可能根本不必錄影，而是更適合進行即時監控。在黑箱方案與即時監控間選擇何者，亦應基於所追求的目的決定。例如，若影像監控的目的係保存證據，即時方案則通常不適合。有時，較之於儲存有限期間後自動刪除影片，即時監控可能干預性更高（例如，相較於完全沒有顯示器、影片直接儲存在黑箱中，有人不斷觀看顯示器的干預性可能更高）。此種情形下必須遵守資料最小化原則（第5條第1項第c款）。還應謹記，控管者可能不使用影像監控，而是使用能夠直接採取因應與干預措施的保全人員。

3.1.3 Balancing of interests

利益衡平

30. Presuming that video surveillance is necessary to protect the legitimate interests of a controller, a video surveillance system may only be put in operation, if the legitimate interests of the controller or those of a third party (e.g. protection of property or physical integrity) are not overridden by the interests or fundamental rights and freedoms of the data subject. The controller needs to consider 1) to what extent the monitoring affects interests, fundamental rights and freedoms of individuals and 2) if this causes violations or negative consequences with regard to the data subject's rights. In fact, balancing the interests is mandatory. Fundamental rights and freedoms on one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully.

假設影像監控是保護控管者正當利益的必要措施，則唯有控管者或

第三方的正當利益（例如保護財產或人身安全）未被當事人之利益或基本權利與自由超越時，方可啟用影像監控系統。控管者需要考慮：1）監控在多大程度上影響個人之利益、基本權利與自由；以及2）是否侵害當事人之權利或有不利影響。事實上，利益衡平是強制要求。必須審慎評估和衡平基本權利與自由，以及控管者的正當利益。

31.

Example: A private parking company has documented reoccurring problems with thefts in the cars parked. The parking area is an open space and can be easily accessed by anyone, but is clearly marked with signs and road blockers surrounding the space. The parking company have a legitimate interest (preventing thefts in the customer's cars) to monitor the area during the time of day that they are experiencing problems. Data subjects are monitored in a limited timeframe, they are not in the area for recreational purposes and it is also in their own interest that thefts are prevented. The interest of the data subjects not to be monitored is in this case overridden by the controller's legitimate interest.

示例：一家私有停車場公司已記錄反復發生的車內竊盜事故。該停車場為開放空間，任何人都可輕易進入，但該停車場有明確標誌，周圍設有路障。該停車場公司在發生問題的時段內，對監控該空間有正當利益（防範對客戶之車內竊盜行為）。當事人在有限時段內受監控，他們並非為娛樂目的進入該區域，防範竊盜亦符合他們自己的利益。此時，控管者的正當利益超越當事人不受監控的利益。

Example: A restaurant decides to install video cameras in the restrooms to control the tidiness of the sanitary facilities. In this case the rights of the data subjects clearly overrides the interest of the controller, therefore cameras cannot be installed there.

示例：一家餐館決定在洗手間裝設攝影機，以確保衛生設備的整潔。此時，當事人之權利顯然超越控管者的利益，因此不得在此裝設攝影機。

3.1.3.1 *Making case-by-case decisions*

進行個案判斷

32. As the balancing of interests is mandatory according to the regulation, the decision has to be made on a case-by-case basis (see Article 6 (1) (f)). Referencing abstract situations or comparing similar cases to one another is insufficient. The controller has to evaluate the risks of the intrusion of the data subject's rights; here the decisive criterion is the intensity of intervention for the rights and freedoms of the individual.

由於「規則」強制要求利益衡平，必須進行個案判斷（見第6條第1項第f款）。援用抽象情形或類比相似案例並不足夠。控管者必須評估干預當事人權利之風險；此處的判斷標準是對該個人權利與自由之干預強度。

33. Intensity can inter alia be defined by the type of information that is gathered (information content), the scope (information density, spatial and geographical extent), the number of data subjects concerned, either as a specific number or as a proportion of the relevant population, the situation in question, the actual interests of the group of data subjects, alternative means, as well as by the nature and scope of the data assessment.

強度可尤其（inter alia）以如下要素界定：所蒐集資訊之類型（資訊內容），範圍（資訊密度、空間與地理範圍），所涉當事人之數量（具體數目或在相關人群中所佔比例），所涉具體情況，當事人群體之真實利益，替代方法，以及資料評估之性質與範圍。

34. Important balancing factors can be the size of the area, which is under surveillance and the amount of data subjects under surveillance. The use of video surveillance in a remote area (e.g. to watch wildlife or to protect critical infrastructure such as a privately owned radio antenna) has to be assessed differently than video surveillance in a pedestrian zone or a shopping mall.

重要的衡平要素可能是：受監控區域的面積，以及受監控當事人之數目。在偏遠地區使用影像監控（例如觀察野生動物，或保護私有無線電天線等關鍵基礎設施）之評估，必須有別於在行人徒步區或購物中心實施影像監控之評估。

35.

Example: If a dash cam is installed (e. g. for the purpose of collecting evidence in case of an accident), it is important to ensure that this camera is not constantly recording traffic, as well as persons who are near a road. Otherwise the interest in having video recordings as evidence in the more theoretical case of a road accident cannot justify this serious interference with data subjects' rights.^{11**}

示例：若已安裝行車記錄器（例如為事故蒐證目的），重要的是確保該記錄器不會持續攝錄交通以及路邊人員。否則，在道路事故之假想情況下以錄影為證據的利益，不得作為嚴重干預當事人權利之正當理由^{11**}。

3.1.3.2 *Data subjects' reasonable expectations*

當事人之合理期待

36. According to Recital 47, the existence of a legitimate interest needs careful assessment. Here the reasonable expectations of the data subject at the time and in the context of the processing of its personal data have to be included. Concerning systematic monitoring, the relationship between data subject and controller may vary significantly and may affect what reasonable expectations the data subject might have. The interpretation of the concept of reasonable expectations should not only be based on the subjective expectations in question. Rather, the decisive criterion has to be if an objective third party could reasonably expect and conclude to be subject to monitoring in this specific situation.

依前言第47點，正當利益是否存在需要審慎評估。此時，必須納入當事人在其個資運用當時之合理期待。關於系統性監控，當事人和控管者間的關係可能有重大區別，並可能影響當事人所抱持的合理期待。合理期待這一概念的解釋不應僅基於所涉當事人的主觀期待。相反，決定性標準應是客觀第三方在該特定情形下，可否合理期待並決定受監控。

37. For instance, an employee in his/her workplace is in most cases not likely expecting to be monitored by his or her employer.¹² Furthermore, monitoring is not to be expected in one's private garden, in living areas,

or in examination and treatment rooms. In the same vein, it is not reasonable to expect monitoring in sanitary or sauna facilities – monitoring such areas is an intense intrusion into the rights of the data subject. The reasonable expectations of data subjects are that no video surveillance will take place in those areas. On the other hand, the customer of a bank might expect that he/she is monitored inside the bank or by the ATM.

例如，大部分情況下，員工不期待在其工作場所被僱主監控¹²。此外，在私人花園、起居場所，或診察或治療室，也不期待被監控。同樣地，衛生或桑拿設施中受監控之期待並不合理—監控這些區域係對當事人權利之重大干預。當事人合理期待這些區域不會進行影像監控。另一方面，銀行的客戶可能期待其在銀行內部或ATM中被監控。

38. Data subjects can also expect to be free of monitoring within publicly accessible areas especially if those areas are typically used for recovery, regeneration, and leisure activities as well as in places where individuals stay and/or communicate, such as sitting areas, tables in restaurants, parks, cinemas and fitness facilities. Here the interests or rights and freedoms of the data subject will often override the controller's legitimate interests.

當事人還可能期待在公眾開放區域不受監控，特別是當這些區域通常用於恢復、放鬆與休閒活動，以及個人逗留和（或）交流之場所，例如休息區、餐廳的餐桌、公園、電影院和健身設備。此時，當事人之利益或權利與自由通常超越控管者的正當利益。

39.

Example: In toilets data subjects expect not to be monitored. Video surveillance for example to prevent accidents is not proportional.

示例：當事人期待在廁所裡不受監控。為防範事故等目的實施影像監控不合比例。

40. Signs informing the data subject about the video surveillance have no

**譯註：原文此處註11無內容，應為誤植。

¹² See also: Article 29 Working Party, Opinion 2/2017 on data processing at work, WP249, adopted on 8 June 2017.

另見：第29條工作小組，關於職業環境的資料運用之意見2/2017（WP249），2017年6月8日通過。

relevance when determining what a data subject objectively can expect. This means that e.g. a shop owner cannot rely on customers objectively having reasonable expectations to be monitored just because a sign informs the individual at the entrance about the surveillance.

在確定當事人的客觀期待時，設立告示牌告知當事人存在影像監控並非相關要素。這意味著，例如，店主不能僅基於入口處設有告示牌告知人們存在監控，即主張顧客客觀期待受監控。

3.2 Necessity to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, Article 6 (1) (e)

為執行符合公共利益之職務或控管者受託行使公權力所必要，
第6條第1項第e款

41. Personal data could be processed through video surveillance under Article 6 (1) (e) if it is necessary to perform a task carried out in the public interest or in the exercise of official authority.¹³ It may be that the exercise of official authority does not allow for such processing, but other legislative bases such as “health and safety” for the protection of visitors and employees may provide limited scope for processing, while still having regard for GDPR obligations and data subject rights.

為執行符合公共利益之職務或行使公權力所必要時，得依據第6條第1項第e款以影像監控運用個人資料¹³。可能的情形是，行使公權力並不允許此等運用，但其他法律依據，例如保護來訪者和員工的「健康和 safety」，可能允許有限範圍之運用，而仍遵守GDPR義務和當事人權利。

42. Member States may maintain or introduce specific national legislation for video surveillance to adapt the application of the rules of the GDPR by determining more precisely specific requirements for processing as long as it is in accordance with the principles laid down by the GDPR (e.g. storage limitation, proportionality).

會員國得為影像監控維持或提出特定國家立法，在符合GDPR所定原

¹³ The basis for the processing referred shall be laid down by Union law or Member State law» and «shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 (3)).

此一運用依據應由歐盟法律或會員國法律規定，「且」係為執行符合公共利益之職務或行使控管者已被賦予之公權力所必要（第6條第3項）。

則（例如儲存限制、比例原則）的前提下，更精確地確定運用之具體要求，調整GDPR規則之適用。

3.3 Consent, Article 6 (1) (a)

同意，第6條第1項第a款

43. Consent has to be freely given, specific, informed and unambiguous as described in the guidelines on consent.¹⁴

如同意指引所述，同意必須自主給予、特定、知情且非模糊¹⁴。

44. Regarding systematic monitoring, the data subject's consent can only serve as a legal basis in accordance with Article 7 (see Recital 43) in exceptional cases. It is in the surveillance's nature that this technology monitors an unknown number of people at once. The controller will hardly be able to prove that the data subject has given consent prior to processing of its personal data (Article 7 (1)). Assumed that the data subject withdraws its consent it will be difficult for the controller to prove that personal data is no longer processed (Article 7 (3)).

關於系統性監控，僅有在符合第7條的特殊情形下（見前言第43點），方可援用當事人的同意作為法律依據。依監控之本質，該技術同時監控不特定數目之人。控管者將幾乎無法證明當事人在其個資被運用前已給予同意（第7條第1項）。假設當事人撤回同意，控管者將很難證明不再運用該個資（第7條第3項）。

45.

Example: Athletes may request monitoring during individual exercises in order to analyse their techniques and performance. On the other hand, where a sports club takes the initiative to monitor a whole team for the same purpose, consent will often not be valid, as the individual athletes may feel pressured into giving consent so that their refusal of consent does not adversely affect teammates.

示例：運動員可能要求監控個人訓練，以便分析其技巧與表現。另一方面，若運動俱樂部為同樣目的對整支隊伍實施監控，則同意通常是無效的，因為運動員個人可能覺得不得不給予同意，以免拒絕

¹⁴ In addition, the Article 29 Working Party (Art. 29 WP) adopted „Guidelines on consent under Regulation 2016/679“ (WP 259 rev. 01) . - endorsed by the EDPB

此外，第29條工作小組（Art. 29 WP）通過了「關於第2016/679號規則（GDPR）中的同意之指引」（WP 259 rev. 01），EDPB採認。

46. If the controller wishes to rely on consent it is his duty to make sure that every data subject who enters the area which is under video surveillance has given her or his consent. This consent has to meet the conditions of Article 7. Entering a marked monitored area (e.g. people are invited to go through a specific hallway or gate to enter a monitored area), does not constitute a statement or a clear affirmative action needed for consent, unless it meets the criteria of Article 4 and 7 as described in the guidelines on consent.¹⁵

若控管者想要援引同意，則其有責任確保進入該區域的每個當事人皆給予同意¹⁵。此等同意必須符合第7條規定之條件。除非滿足同意指引所論述的第4條和第7條之標準，否則進入標示為受監控之區域（例如，人們受邀通過特定走廊或大門進入受監控區域），並不構成同意所必需之聲明或「清楚肯定行為」。

47. Given the imbalance of power between employers and employees, in most cases employers should not rely on consent when processing personal data, as it is unlikely to be freely given. The guidelines on consent should be taken into consideration in this context.

考量到僱主和員工間權利不對等，大部分情形下，僱主不應援引同意運用個人資料，因為同意不太可能係自主給予。此時，應考慮同意指引的內容。

48. Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context (see Article 88).

會員國法律或團體協約，包括「工會協約」，可能為僱傭關係中運用員工之個人資料規定具體規則（見第88條）。

¹⁵ In addition, the Article 29 Working Party (Art. 29 WP) adopted „Guidelines on consent under Regulation 2016/679“ (WP 259) - endorsed by the EDPB - which should be taken in account.

此外，還應考慮第29條工作小組（Art. 29 WP）通過之「關於第2016/679號規則（GDPR）中的同意之指引」（WP 259 rev. 01），EDPB採認。

4 DISCLOSURE OF VIDEO FOOTAGE TO THIRD PARTIES

向第三方揭露影片

49. In principle, the general regulations of the GDPR apply to the disclosure of video recordings to third parties.

原則上，GDPR之一般規則適用於向第三方揭露影片。

4.1 Disclosure of video footage to third parties in general

向第三方揭露影片概述

50. Disclosure is defined in Article 4 (2) as transmission (e.g. individual communication), dissemination (e.g. publishing online) or otherwise making available. Third parties are defined in Article 4 (10). Where disclosure is made to third countries or international organisations, the special provisions of Article 44 et seq. also apply.

第4條第2款將揭露定義為傳輸（例如個人通訊）、散播（例如線上公開）或以其他方式提供。第4條第10款定義了第三方。向第三國或國際組織揭露時，還適用第44條以下的特殊規定。

51. Any disclosure of personal data is a separate kind of processing of personal data for which the controller needs to have a legal basis in Article 6.

任何揭露個資的行為都是對個資的獨立運用，控管者需要具備第6條規定的法律依據。

52.

Example: A controller who wishes to upload a recording to the Internet needs to rely on a legal basis for that processing, for instance by obtaining consent from the data subject according to Article 6 (1) (a).

示例：控管者想要將影片上傳至網路，需要對此運用援引法律依據，例如依第6條第1項第a款獲得當事人同意。

53. The transmission of video footage to third parties for the purpose other than that for which the data has been collected is possible under the rules of Article 6 (4).

依第6條第4項，得為不同於該資料蒐集之原始目的的其他目的，向第三方傳輸影片。

54.

Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. A damage occurs and the recording is transferred to a lawyer to pursue a case. In this case the purpose for recording is the same as the one for transferring.

示例：為處理故意破壞行為之目的，對（停車場）路障裝設影像監控。破壞行為發生後，影片被交予律師進行求償。此時錄影之目的與移轉影片之目的相同。

Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. The recording is published online for pure amusement reasons. In this case the purpose has changed and is not compatible with the initial purpose. It would furthermore be problematic to identify a legal basis for that processing (publishing).

示例：為處理故意破壞行為之目的，對（停車場）路障裝設影像監控。該影片為單純娛樂目的被公開於網路。此時，目的已改變，與原始目的不符。識別此一運用（公開）之法律依據進而成為問題。

55. A third party recipient will have to make its own legal analysis, in particular identifying its legal basis under Article 6 for his processing (e.g. receiving the material).

第三方接收者本身必須進行法律分析，特別是依第6條識別其運用（例如接收該影片）之法律依據。

4.2 Disclosure of video footage to law enforcement agencies

向執法機關揭露影片

56. The disclosure of video recordings to law enforcement agencies is also an independent process, which requires a separate justification for the controller.

向執法機關揭露影片也是一項獨立運用，控管者對此另行需要正當理由。

57. According to Article 6 (1) (c), processing is legal if it is necessary for compliance with a legal obligation to which the controller is subject. Although the applicable police law is an affair under the sole control of the Member States, there are most likely general rules that regulate the transfer of evidence to law enforcement agencies in every Member State. The processing of the controller handing over the data is regulated by

the GDPR. If national legislation requires the controller to cooperate with law enforcement (e. g. investigation), the legal basis for handing over the data is legal obligation under Article 6 (1) (c).

依據第6條第1項第c款，運用若係履行控管者負有的法定義務所必要，則為合法。雖然可適用的警察法為會員國自主管控之事務，每個會員國很可能設有規範向執法機關移交證據之一般規則。控管者交出資料之運用行為受GDPR規範。若國家立法要求控管者配合執法（例如調查），則交出資料之法律依據為第6條第1項第c款之法定義務。

58. The purpose limitation in Article 6 (4) is then often unproblematic, since the disclosure explicitly goes back to Member State law. A consideration of the special requirements for a change of purpose in the sense of lit. a - e is therefore not necessary.

此時，由於揭露明確回歸到會員國法律，第6條第4項規定的目的限制通常不會有問題。因此無需考慮第a款至第e款關於變更目的之特殊要求。

59.

Example: A shop owner records footage at its entrance. The footage shows a person stealing another person's wallet. The police asks the controller to hand over the material in order to assist in their investigation. In that case the shop owner would use the legal basis under Article 6 (1) (c) (legal obligation) read in conjunction with the relevant national law for the transfer processing.

示例：一名店主在入口處錄影。影片顯示一個人在偷竊他人錢包。警方要求控管者交出影片，以協助其調查。此時，控管者對此移交運用行為，得使用第6條第1項第c款（法定義務）連結相關國內法為法律依據。

60.

Example: A camera is installed in a shop for security reasons. The shop owner believes he has recorded something suspicious in his footage and decides to send the material to the police (without any indication that there is an ongoing investigation of some kind). In this case the shop owner has to assess whether the conditions under, in most cases, Article 6 (1) (f) are met. This is usually the case if the shop owner has a

reasonable suspicion of that a crime has been committed.

示例：一家商店為安全原因裝設攝影機。店主認為其錄到了可疑行為，並將影片發送給警方（而無跡象表明正在進行某種調查）。此時，大部分情形下，店主須評估是否符合第6條第1項第f款規定之條件。若店主合理懷疑已實施犯罪，則通常屬於此情形。

61. The processing of the personal data by the law enforcement agencies themselves does not follow the GDPR (see Article 2 (2) (d)), but follows instead the Law Enforcement Directive (EU2016/680).

執法機關本身對個人資料之運用不適用GDPR（見第2條第2項第d款），而是適用執法指令（EU2016/680）。

5 PROCESSING OF SPECIAL CATEGORIES OF DATA

運用特種個資

62. Video surveillance systems usually collect massive amounts of personal data which may reveal data of a highly personal nature and even special categories of data. Indeed, apparently non-significant data originally collected through video can be used to infer other information to achieve a different purpose (e.g. to map an individual's habits). However, video surveillance is not always considered to be processing of special categories of personal data.

影像監控系統通常蒐集巨量的個人資料，且可能揭示高度私人性質之資料，甚至特種個資。事實上，影片初始蒐集看似不重要的資料可能用以推斷實現不同目的的其他資訊（例如剖繪個人習慣）。然而，影像監控並非總是構成對特種個資的運用。

63.

Example: Video footage showing a data subject wearing glasses or using a wheel chair are not per se considered to be special categories of personal data.

示例：影片顯示當事人戴眼鏡或使用輪椅並不當然屬於特種個資。

64. However, if the video footage is processed to deduce special categories of data Article 9 applies.

然而，若影片被用於推斷特種個資，則適用第9條。

65.

Example: Political opinions could for example be deduced from images showing identifiable data subjects taking part in an event, engaging in a strike, etc. This would fall under Article 9.

示例：從可得識別之當事人出席活動、參加罷工等畫面，可推知其政治立場。這將適用第9條。

Example: A hospital installing a video camera in order to monitor a patient's health condition would be considered as processing of special categories of personal data (Article 9).

示例：醫院裝設攝影機，以監控病患的健康狀況，這構成運用特種個資（第9條）。

66. In general, as a principle, whenever installing a video surveillance system

careful consideration should be given to the data minimization principle. Hence, even in cases where Article 9 (1) does not apply, the data controller should always try to minimize the risk of capturing footage revealing other sensitive data (beyond Article 9), regardless of the aim.

一般而言，作為一項原則，在裝設影像監控系統時，均應審慎考慮資料最小化原則。因此，即使在不適用第9條第1項的情況下，無論其目的如何，資料控管者應總是盡力降低影片揭示（第9條之外的）其他敏感資料之風險。

67.

Example: Video surveillance capturing a church does not per se fall under Article 9. However, the controller has to conduct an especially careful assessment under Article 6 (1) (f) taken into account the nature of the data as well as the risk of capturing other sensitive data (beyond Article 9) when assessing the interests of the data subject.

示例：對教堂的影像監控並不當然適用第9條。然而，控管者在評估當事人的利益時，必須考量資料之性質與拍攝到（第9條之外的）其他敏感資料之風險，依第6條第1項第f款進行審慎評估。

68. If a video surveillance system is used in order to process special categories of data, the data controller must identify both an exception for processing special categories of data under Article 9 (i.e. an exemption from the general rule that one should not process special categories of data) and a legal basis under Article 6.

若影像監控系統係用於運用特種個資，資料控管者必須同時識別第9條規定的運用特種個資之例外（亦即，不得運用特種個資之一般原則的例外），以及第6條規定之法律依據。

69. For instance, Article 9 (2) (c) (“[...] processing is necessary to protect the vital interests of the data subject or of another natural person [...]”) could – in theory and exceptionally – be used, but the data controller would have to justify it as an absolute necessity to safeguard the vital interests of a person and prove that this “[...] data subject is *physically or legally incapable of giving his consent*.”. In addition, the data controller won’t be allowed to use the system for any other reason.

例如，第9條第2項第c款（「……運用係為保護當事人或其他自然人之重大利益所必要……」）能夠——理論上且例外地——用於此處，但

資料控管者必須論證此為保護相關人員重大利益之絕對必要，且證明「……當事人身體上或法律上無法給予同意……」。此外，資料控管者不得為其他理由使用此系統。

70. It is important to note here that every exemption listed in Article 9 is not likely to be usable to justify processing of special categories of data through video surveillance. More specifically, data controllers processing those data in the context of video surveillance cannot rely on Article 9 (2) (e), which allows processing that relates to personal data that are manifestly made public by the data subject. The mere fact of entering into the range of the camera does not imply that the data subject intends to make public special categories of data relating to him or her.

重要的是，此處應注意，第9條所列各項例外不太可能被用作以影像監控運用特種個資的正當理由。具體而言，資料控管者以錄影監控運用此類資料，不得援用第9條第2項第e款，該款允許運用當事人明顯已自行公開之資料。進入攝影機攝錄範圍的單純事實並不意味著當事人有意公開其特種個資。

71. Furthermore, processing of special categories of data requires a heightened and continued vigilance to certain obligations; for example high level of security and data protection impact assessment where necessary.

此外，運用特種個資需要對特定義務有更高程度及持續的警覺；例如高度安全保護、必要時辦理個資保護影響評估。

72.

Example: An employer must not use video surveillance recordings showing a demonstration in order to identify strikers.

示例：僱主不得使用罷工遊行之監控錄影識別罷工者。

5.1 General considerations when processing biometric data

運用生物特徵資料之一般考量

73. The use of biometric data and in particular facial recognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as

particularly effective, controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing.

使用生物特徵資料，特別是臉部辨識，將提高當事人權利之風險。關鍵是在援用此類技術時，充分尊重GDPR所規定的合法性、必要性、合乎比例和資料最小化等原則。儘管使用此等技術可能被認為特別有效，控管者應首先評估對基本權利與自由之影響，並考慮以干預性較低的手段實現其運用之正當目的。

74. To qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a measurement of this characteristics. Since biometric data is the result of such measurements, the GDPR states in its Article 4.14 that it is “[...] *resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person [...]*”. The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual.¹⁶

構成GDPR所定義的生物特徵資料的條件為，對於原始資料（例如自然人的身體、生理或行為特徵）的運用，必須隱含對此等特徵之評量。由於生物特徵資料係這種評量之結果，GDPR在第4條第14款規定，其係「……對自然人身體、生理或行為特徵之特定技術運用，以實現或確認對該自然人的獨特性識別……」。然而，若未將某一個人之影片作特定技術運用，以協助識別該個人，則該影片本身不構成第9條規定的生物特徵資料¹⁶。

75. In order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed “for the purpose of uniquely identifying a natural person”.

¹⁶ Recital 51 supports this analysis, stating that “[...] *The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. [...]*”.

前言第51點支持這一分析，認為「……運用照片不應一概被視為運用特種個資，因為只有在運用係以特定技術方法為之，且能夠獨特性識別或認證某一自然人時，其才落入生物特徵資料的定義範圍……」。

構成運用特種個資（第9條）之條件為，係「為獨特性識別自然人目的」而運用生物特徵資料。

76. To sum up, in light of Article 4.14 and 9, three criteria must be considered:

概言之，依第4條第14款和第9條，必須考量三項標準：

- **Nature of data** : data relating to physical, physiological or behavioural characteristics of a natural person,
資料性質：資料係關於自然人的身體、生理或行為特徵，
- **Means and way of processing** : data “resulting from a specific technical processing”,
運用方法和方式：資料係「特定技術運用之結果」，
- **Purpose of processing**: data must be used for the purpose of uniquely identifying a natural person.
運用目的：資料必須以用於獨特性識別自然人為目的。

77. The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require explicit consent from all data subjects (Article 9 (2) (a)), however another suitable exception in Article 9 could also be applicable.

私人實體為其本身目的（例如行銷、統計，甚至保全），運用其所裝設的包含生物特徵辨識功能的影像監控裝置，將在大部分情況下需要全部當事人之明確同意（第9條第2項第a款），而第9條規定的其他適當例外也可能適用。

78.

Example: To improve its service a private company replaces passenger identification check points within an airport (luggage drop-off, boarding) with video surveillance systems that use facial recognition techniques to verify the identity of the passengers that have chosen to consent to such a procedure. Since the processing falls under Article 9, the passengers, who will have previously given their explicit and informed consent, will have to enlist themselves at for example an automatic terminal in order to create and register their facial template associated with their boarding pass and identity. The check points with facial recognition need

to be clearly separated, e. g. the system must be installed within a gantry so that the biometric templates of non-consenting person will not be captured. Only the passengers, who will have previously given their consent and proceeded with their enrolment, will use the gantry equipped with the biometric system.

示例：為提升服務，一家私人公司以影像監控系統代替了機場內旅客身分查驗點（托運行李、登機），對於同意這一作業的旅客，運用臉部辨識技術查驗其身分。由於此等運用適用第9條，旅客須事先給予明確知情同意後，必須主動前往自動終端等設施，創設並登錄與其登機證和身分相關之臉部模板。臉部識別查驗點應作明確區分，例如，該系統應裝設門架（gantry），以免拍攝未給予同意人員的生物辨識模板。唯有已給予同意並進行登錄的旅客將使用裝設生物辨識系統的門架。

Example: A controller manages access to his building using a facial recognition method. People can only use this way of access if they have given their explicitly informed consent (according to Article 9 (2) (a)) beforehand. However, in order to ensure that no one who has not previously given his or her consent is captured, the facial recognition method should be triggered by the data subject himself, for instance by pushing a button. To ensure the lawfulness of the processing, the controller must always offer an alternative way to access the building, without biometric processing, such as badges or keys.

示例：一名控管者使用臉部辨識方法進行門禁管理。唯有事前給予明確知情同意（依第9條第2項第a款）的人員方可使用此通行方式。然而，為確保避免拍攝未事先同意之人，該臉部辨識方法應由當事人自己啟動，例如通過按鈕等方式。為確保運用之合法性，控管者必須隨時提供不涉及生物特種運用的替代通行方式，例如門卡或鑰匙。

79. In this type of cases, where biometric templates are generated, controllers shall ensure that once a match or no-match result has been obtained, all the intermediate templates made on the fly (with the explicit and informed consent of the data subject) in order to be compared to the ones created by the data subjects at the time of the enlistment, are immediately and securely deleted. The templates

created for the enlistment should only be retained for the realisation of the purpose of the processing and should not be stored or archived.

此類案例中，若生成生物特徵模板，在獲得匹配或不匹配之結果後，對於為了與當事人加入系統時創設的模版相比對而製作的臨時模版（經當事人明確知情同意），控管者應確保立即以安全方式將其刪除。加入系統時創設之模版，其保存期間應以實現運用目的為限，而不得被儲存或建檔。

80. However, when the purpose of the processing is for example to distinguish one category of people from another but not to uniquely identify anyone the processing does not fall under Article 9.

然而，若運用是為了區分某一類人等目的，而非獨特性識別某個人，則其不適用第9條。

81.

Example: A shop owner would like to customize its advertisement based on gender and age characteristics of the customer captured by a video surveillance system. If that system does not generate biometric templates in order to uniquely identify persons but instead just detects those physical characteristics in order to classify the person then the processing would not fall under Article 9 (as long as no other types of special categories of data are being processed).

示例：一名店主想要根據影像監控系統攝錄到的顧客性別和年齡特徵客製其廣告。若該系統並不生成用以獨特性識別個人的生物特徵模板，而是為客群分類目的偵測此等生理特徵，則其運用不適用第9條（在不運用其他特種個資的前提下）。

82. However, Article 9 applies if the controller stores biometric data (most commonly through templates that are created by the extraction of key features from the raw form of biometric data (e.g. facial measurements from an image)) in order to uniquely identify a person. If a controller wishes to detect a data subject re-entering the area or entering another area (for example in order to project continued customized advertisement), the purpose would then be to uniquely identify a natural person, meaning that the operation would from the start fall under Article 9. This could be the case if a controller stores generated templates to provide further tailored advertisement on several

billboards throughout different locations inside the shop. Since the system is using physical characteristics to detect specific individuals coming back in the range of the camera (like the visitors of a shopping mall) and tracking them, it would constitute a biometric identification method because it is aimed at recognition through the use of specific technical processing.

然而，若控管者為獨特性識別個人而儲存生物特徵資料（通常是從原始形式的生物特徵資料（例如圖像中的臉部測量值）中提取出關鍵特徵並創設模板），則適用第9條。若控管者想要偵測一名當事人重新進入該區域或進入其他區域（例如，為了持續投放客製化廣告目的），則其目的係獨特性識別自然人，意味著此等作業自始即適用第9條。若控管者儲存所生成的模板，以便在店內不同位置的數個廣告牌上投放客製化程度更高的廣告，即屬於此情形。由於該系統係運用生理特徵偵測特定個人返回攝像機的攝錄範圍內（比如進入賣場之人）並追蹤該個人，則將構成生物特徵辨識方法，因為其目的在於透過特定技術運用進行識別。

83.

Example: A shop owner has installed a facial recognition system inside his shop in order to customize its advertisement towards individuals. The data controller has to obtain the explicit and informed consent of all data subjects before using this biometric system and delivering tailored advertisement. The system would be unlawful if it captures visitors or passers-by who have not consented to the creation of their biometric template, even if their template is deleted within the shortest possible period. Indeed, these temporary templates constitute biometric data processed in order to uniquely identify a person who may not want to receive targeted advertisement.

示例：一名店主在其店內安裝臉部辨識系統，以便向特定個人投放客製化廣告。資料控管者必須在使用這一生物特徵系統並投放客製化廣告前，獲得全部當事人之明確知情同意。若該系統拍攝到尚未給予同意的訪客或路人，並製作其生物特徵模板，則即使在極短時間內刪除該模板，亦不合法。實際上，這些臨時模板構成為獨特性識別個人而運用之生物特徵資料，而被識別之個人可能不願意接收定向廣告。

84. The EDPB observes that some biometric systems are installed in uncontrolled environments¹⁷, which means that the system involves capturing on the fly the faces of any individual passing in the range of the camera, including persons who have not consented to the biometric device, and thereby creating biometric templates. These templates are compared to the ones created of data subjects having given their prior consent during an enlistment process (i.e. a biometric device user) in order for the data controller to recognise whether the person is a biometric device user or not. In this case, the system is often designed to discriminate the individuals it wants to recognize from a database from those who are not enlisted. Since the purpose is to uniquely identify natural persons, an exception under Article 9 (2) GDPR is still needed for anyone captured by the camera.

EDPB觀察到，某些生物特徵系統裝設於不受控之環境¹⁷，這意味著該系統涉及一併拍攝進入攝影機範圍內的任何個人（包括尚未同意生物特徵裝置之人）之臉部，並創設其生物特徵模板。這些模板與已事先同意之當事人加入系統時（亦即生物特徵裝置使用者）所創設的模板相比對，從而使資料控管者識別其是否為生物特徵裝置使用者。此時，系統通常設計為區分想從資料庫被識別之人與尚未加入系統之人。由於其目的是獨特性識別自然人，對於攝影機拍攝到的任何人，都仍需要援用GDPR第9條第2項規定的例外。

85.

Example: A hotel uses video surveillance to automatically alert the hotel manager that a VIP has arrived when the face of the guest is recognized. These VIPs have priorly given their explicit consent to the use of facial recognition before being recorded in a database established for that purpose. These processing systems of biometric data would be unlawful unless all other guests monitored (in order to identify the VIPs) have consented to the processing according to Article 9 (2) (a) GDPR.

¹⁷ It means that the biometric device is located in a space open to the public and is able to work on anyone passing by, as opposed to the biometric systems in controlled environments that can be used only by consenting person's participation.

意指生物特徵裝置放置於公眾開放空間內，且能夠對任何路過之人使用，而不是位於受控環境中，僅對同意參與之人使用。

示例：一家旅館使用影像監控系統，在臉部辨識出VIP客人後，自動提示旅館經理一位VIP客人已抵達。這些VIP客人在其錄入相關資料庫前，已對臉部辨識給予事先明確同意。除非（為識別VIP客人而）受監控的其他客人全都依GDPR第9條第2項第a款同意此運用，否則該生物特徵資料運用系統並不合法。

Example: A controller installs a video surveillance system with facial recognition at the entrance of the concert hall he manages. The controller must set up clearly separated entrances; one with a biometric system and one without (where you instead for example scan a ticket). The entrances equipped with biometric devices, must be installed and made accessible in a way that prevents the system from capturing biometric templates of non-consenting spectators.

示例：一名控管者在其管理的音樂廳入口處裝設附有臉部辨識功能的影像監控系統。該控管者必須設置彼此明確區隔的不同入口，一個設有生物特徵系統，另一個則沒有（通過掃描票券等方式入場）。設有生物特徵系統的入口的裝設與提供方式，必須避免該系統拍攝未同意觀眾之生物特徵模板。

86. Finally, when the consent is required by Article 9 GDPR, the data controller shall not condition the access to its services to the acceptance of the biometric processing. In other words and notably when the biometric processing is used for authentication purpose, the data controller must offer an alternative solution that does not involve biometric processing – without restraints or additional cost for the data subject. This alternative solution is also needed for persons who do not meet the constraints of the biometric device (enrolment or reading of the biometric data impossible, disability situation making it difficult to use, etc.) and in anticipation of unavailability of the biometric device (such as a malfunction of the device), a "back-up solution" must be implemented to ensure continuity of the proposed service, limited however to exceptional use. In exceptional cases, there might be a situation where processing biometric data is the core activity of a service provided by contract, e.g. a museum that sets up an exhibition to demonstrate the use of a facial recognition device, in which case the data subject will not be able to reject the processing of biometric data should they wish to participate in the exhibition. In such case the

consent required under Article 9 is still valid if the requirements in Article 7 are met.

最後，當依GDPR第9條要求獲得同意，資料控管者不得將接受生物特徵運用作為獲取其服務之前提條件。換言之，特別是當為認證目的運用生物特徵時，資料控管者必須提供不涉及生物特徵運用之替代方案—而不得限制當事人或增加其成本。對於未符合生物特徵裝置限制條件之人（無法登錄或讀取生物特徵資料，因身心障礙而難以使用等），以及預料生物特徵裝置不可用的情形（如裝置故障），亦應提供替代方案。必須設置「備選方案」，以確保所涉服務之持續性，雖然其僅限於例外使用。在例外情形下，運用生物特徵資料可能係依契約提供之服務的核心活動，例如，博物館籌備一項展覽，展示臉部辨識裝置之使用，此時，若當事人想要參與該展覽，則不得拒絕運用生物特徵資料。此時，若符合第7條的要求，則第9條規定的同意仍為有效。

5.2 Suggested measures to minimize the risks when processing biometric data

運用生物特徵資料時將風險降到最小之建議措施

87. In compliance with the data minimization principle, data controllers must ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, thereby avoiding any possible further processing. Measures should be put in place to guarantee that templates cannot be transferred across biometric systems.

依資料最小化原則，資料控管者必須確保，為構建模板而從數位圖像中提取之資料不得過度，且僅包含為該特定目的所必需之資訊，從而避免任何潛在的進階運用。應採取措施確保模板無法在生物特徵系統間移轉。

88. Identification and authentication/verification are likely to require the storage of the template for use in a later comparison. The data controller must consider the most appropriate location for storage of the data. In an environment under control (delimited hallways or checkpoints), templates shall be stored on an individual device kept by the user and under his or her sole control (in a smartphone or the id card) or – when needed for specific purposes and in presence of objective

needs – stored in a centralized database in an encrypted form with a key/secret solely in the hands of the person to prevent unauthorised access to the template or storage location. If the data controller cannot avoid having access to the templates, he must take appropriate steps to ensure the security of the data stored. This may include encrypting the template using a cryptographic algorithm.

識別和認證/驗證可能要求儲存模板，以便用於後續比對。資料控管者必須考量儲存資料最適當的位置。在可控環境下（限定走道或查驗點），模板應儲存於由使用者保管且單獨控制的獨立裝置（智慧型手機或身分識別證）上，或者—當特定目的需要如此，且存在客觀需求時—以加密形式儲存在集中式資料庫中，且密鑰/加密僅由該人保管，以免未經授權存取模板或儲存位置。若資料控管者不得不存取模板，其必須採取適當步驟確保所儲存資料之安全。這可能包括使用加密演算法為模板加密。

89. In any case, the controller shall take all necessary precautions to preserve the availability, integrity and confidentiality of the data processed. To this end, the controller shall notably take the following measures: compartmentalize data during transmission and storage, store biometric templates and raw data or identity data on distinct databases, encrypt biometric data, notably biometric templates, and define a policy for encryption and key management, integrate an organisational and technical measure for fraud detection, associate an integrity code with the data (for example signature or hash) and prohibit any external access to the biometric data. Such measures will need to evolve with the advancement of technologies.

無論如何，控管者應採取一切必要預防措施，保護所運用資料的可用性、完整性與機密性。為此目的，控管者尤其應採取下列措施：在傳輸與儲存過程中劃分（compartmentalize）資料，將生物特徵模板與原始資料或身分資料儲存於不同資料庫中，加密生物特徵資料（特別是生物特徵模板），定義加密與密鑰管理政策，整合詐欺偵測之組織性和技術性措施，結合資料完整性編碼（例如簽名或雜湊值（hash）），以及禁止外部存取生物特徵資料。這些措施需要隨技術進步而演進。

90. Besides, data controllers should proceed to the deletion of raw data

(face images, speech signals, the gait, etc.) and ensure the effectiveness of this deletion. If there is no longer a lawful basis for the processing, the raw data has to be deleted. Indeed, insofar as biometric templates derives from such data, one can consider that the constitution of databases could represent an equal if not even bigger threat (because it may not always be easy to read a biometric template without the knowledge of how it was programmed, whereas raw data will be the building blocks of any template). In case the data controller would need to keep such data, noise-additive methods (such as watermarking) must be explored, which would render the creation of the template ineffective. The controller must also delete biometric data and templates in the event of unauthorized access to the read-comparison terminal or storage server and delete any data not useful for further processing at the end of the biometric device's life.

此外，資料控管者應刪除原始資料（臉部圖像、語音訊號、步態等），並確保有效刪除。若運用不再有合法依據，必須刪除原始資料。實際上，由於生物特徵模板係由這些資料衍生得出，可以認為構建資料庫係同等（若非更大）威脅（因為若不知生物特徵模板的編程方法，則不易讀取模板，而原始資料則是構建任何模板的基石）。若控管者需要保存這些資料，則必須探究添加雜訊（noise-additive）方法（例如加浮水印），使之無法有效創設模板。若讀取—比對終端或儲存伺服器未經授權而被存取，控管者也必須刪除生物特徵資料和模板，生物特徵裝置使用期限屆滿後，無法再作其他使用的資料，也應一併刪除。

6 RIGHTS OF THE DATA SUBJECT

當事人的權利

91. Due to the character of data processing when using video surveillance some data subject's rights under GDPR serves further clarification. This chapter is however not exhaustive, all rights under the GDPR applies to processing of personal data through video surveillance.

由於使用影像監控運用資料之特性，當事人依GDPR享有的某些權利需要進一步釐清。但本章並非完全列舉，GDPR所規定的一切權利均適用於透過影像監控運用個人資料之行為。

6.1 Right to access

近用權

92. A data subject has the right to obtain confirmation from the controller as to whether or not their personal data are being processed. For video surveillance this means that if no data is stored or transferred in any way then once the real-time monitoring moment has passed the controller could only give the information that no personal data is any longer being processed (besides the general information obligations under Article 13, see *section 7 – Transparency and information obligations*). If however data is still being processed at the time of the request (i.e. if the data is stored or continuously processed in any other way), the data subject should receive access and information in accordance with Article 15.

當事人有權向控管者確認其個人資料是否正被運用。對於影像監控而言，這意味著若不以任何方式儲存或移轉資料，則即時監控之瞬間一旦結束，控管者所提供的資訊只能是不再運用任何個人資料（應同時履行第13條的一般資訊提供義務，見第7節，透明化和資訊提供義務）。然而，若該資料在請求之時仍被運用（亦即，若該資料被儲存或連續地以其他方式運用），則當事人應依第15條獲得存取權限並獲知資訊。

93. There are however, a number of limitations that may in some cases apply in relation to the right to access.

然而，某些情形下，近用權可能適用諸多限制。

- Article 15 (4) GDPR, adversely affect the rights of others
GDPR第15條第4項，對他人權利的不利影響

94. Given that any number of data subjects may be recorded in the same sequence of video surveillance a screening would then cause additional processing of personal data of other data subjects. If the data subject wishes to receive a copy of the material (article 15 (3)), this could adversely affect the rights and freedoms of other data subject in the material. To prevent that effect the controller should therefore take into consideration that due to the intrusive nature of the video footage the controller should not in some cases hand out video footage where other data subjects can be identified. The protection of the rights of third parties should however not be used as an excuse to prevent legitimate claims of access by individuals, the controller should in those cases implement technical measures to fulfil the access request (for example, image-editing such as masking or scrambling). However, controllers are not obliged to implement such technical measures if they can otherwise ensure that they are able to react upon a request under Article 15 within the timeframe stipulated by Article 12 (3).

鑒於同一影像監控影片序列中可能攝錄到數目不確定的當事人，過濾影片將導致對其他當事人個資的額外運用。若當事人想要獲得影片副本（第15條第3項），將對影片中其他當事人之權利與自由造成不利影響。為避免此影響，控管者因此應考慮，由於影片的干預性，在某些情況下，若可識別其他當事人，則不得交出影片。然而，不得以保護第三方權利為藉口，阻止個人的正當近用主張，此時，控管者應採取技術措施滿足近用請求（例如，遮蔽（mask）或加擾（scramble）等圖像編輯技術）。然而，若控管者能夠確保以其他方式在第12條第3項規定的時限內，回應依第15條提出之請求，則其並無義務採取這些技術措施。

- Article 11 (2) GDPR, controller is unable to identify the data subject
GDPR第11條第2項，控管者無法識別當事人

95. If the video footage is not searchable for personal data, (i.e. the controller would likely have to go through a large amount of stored material in order to find the data subject in question) the controller may be unable to identify the data subject.

若無法在該影片中搜尋個人資料（亦即，控管者為了找到相關當事人，可能不得不查找所儲存的大量資料），則控管者可能無法識別該當事人。

96. For these reasons the data subject should (besides identifying themselves including with identification document or in person) in its request to the controller, specify when – within a reasonable timeframe in proportion to the amount of data subjects recorded – he or she entered the monitored area. The controller should notify the data subject beforehand on what information is needed in order for the controller to comply with the request. If the controller is able to demonstrate that it is not in a position to identify the data subject, the controller must inform the data subject accordingly, if possible. In such a situation, in its response to the data subject the controller should inform about the exact area for the monitoring, verification of cameras that were in use etc. so that the data subject will have the full understanding of what personal data of him/her may have been processed.

因此，當事人應（在表明其身分的同時，包括提供身分文件或親自到場）在其對控管者的請求中，說明其何時進入受監控區域，該時段精確度應與所攝錄當事人的數目成比例。控管者應將其為遵循該請求所需之資訊預先告知當事人。若控管者能夠證明其無法識別當事人，在可行的前提下，其必須向當事人為此告知。這種情況下，控管者在對當事人的回應中，應告知受監控的具體區域、確認所使用的攝影機等，以便當事人充分瞭解其哪些個人資料可能已被運用。

97.

Example: If a data subject is requesting a copy of his or her personal data processed through video surveillance at the entrance of a shopping mall with 30 000 visitors per day, the data subject should specify when he or she passed the monitored area within approximately a one-hour-timeframe. If the controller still processes the material a copy of the video footage should be provided. If other data subjects can be identified in the same material then that part of the material should be anonymised (for example by blurring the copy or parts thereof) before giving the copy to the data subject that filed the request.

示例：若當事人請求提供影像監控所運用的其個人資料之副本，而該監控係裝設在每日30,000人經過的賣場門口，則當事人應說明其經過受監控區域的時間，精確到大約1小時內。若控管者仍保留有

該影片，則應提供其副本。若同一影片中可識別其他當事人，則在把該副本提供予提出請求的當事人之前，應將影片的有關部分匿名化（例如，將該副本或其中一部分模糊化）。

Example: If the controller is automatically erasing all footage for example within 2 days, the controller is not able to supply footage to the data subject after those 2 days. If the controller receives a request after those 2 days the data subject should be informed accordingly.

示例：若控管者在一定期間（例如2天）內，自動刪除全部影片，則其無法在2天後向當事人提供影片。若控管者在2天期間經過後收到請求，則應對當事人為此告知。

- Article 12 GDPR, excessive requests
GDPR第12條，過度請求

98. In case of excessive or manifestly unfounded requests from a data subject, the controller may either charge a reasonable fee in accordance with Article 12 (5) (a) GDPR, or refuse to act on the request (Article 12 (5) (b) GDPR). The controller needs to be able to demonstrate the manifestly unfounded or excessive character of the request.

若當事人提出過度或顯無理由之請求，控管者得依GDPR第12條第5項第a款收取合理費用，或拒絕對該請求採取行動（GDPR第12條第5項第b款）。控管者需要能夠證明該請求顯無理由或過度之性質。

6.2 Right to erasure and right to object

刪除權和拒絕權

6.2.1 Right to erasure (Right to be forgotten)

刪除權（被遺忘權）

99. If the controller continues to process personal data beyond real-time monitoring (e.g. storing) the data subject may request for the personal data to be erased under Article 17 GDPR.

若控管者在即時監控之外繼續運用（例如儲存）個人資料，當事人得依GDPR第17條請求刪除個人資料。

100. Upon a request, the controller is obliged to erase the personal data without undue delay if one of the circumstances listed under Article 17 (1) GDPR applies (and none of the exceptions listed under Article 17 (3))

GDPR does). That includes the obligation to erase personal data when they are no longer needed for the purpose for which they were initially stored, or when the processing is unlawful (see also *Section 8 – Storage periods and obligation to erasure*). Furthermore, depending on the legal basis of processing, personal data should be erased:

經此請求後，若適用GDPR第17條第1項規定之數款情形之一（且沒有適用GDPR第17條第3項所列的例外情形），控管者有義務刪除該個人資料，不得無故遲延。這包括當資料對其最初儲存之目的不再需要，或運用不合法時，刪除個人資料之義務（另見第8節，儲存期間和刪除義務）。此外，根據運用的法律依據，下列情形應刪除個人資料：

- *for consent* whenever the consent is withdrawn (and there is no other legal basis for the processing)
對於同意，撤回同意時（且運用無其他法律依據）。
- *for legitimate interest*:
對於正當利益：
 - whenever the data subject exercises the right to object (see *Section 6.2.2*) and there are no overriding compelling legitimate grounds for the processing, or
當事人行使拒絕權時（見第6.2.2節），且並無超越性的必要正當理由可進行運用；或
 - in case of direct marketing (including profiling) whenever the data subject objects to the processing.
行銷（包括剖析）時，當事人拒絕運用。

101. If the controller has made the video footage public (e.g. broadcasting or streaming online), reasonable steps need to be taken in order to inform other controllers (that are now processing the personal data in question) of the request pursuant to Article 17 (2) GDPR. The reasonable steps should include technical measures, taking into account available technology and the cost of implementation. To the extent possible, the controller should notify – upon erasure of personal data – anyone to which the personal data previously have been disclosed, in accordance with Article 19 GDPR.

若控管者已公開影片（例如廣播或線上串流），需要依GDPR第17條

第2項採取合理步驟，將該請求告知其他（正在運用該個人資料之）控管者。該合理步驟應包括技術措施，並考量可用之技術與實施成本。在可行範圍內，控管者應一在刪除個人資料後一依GDPR第19條通知已向其揭露該個人資料之任何人。

102. Besides the controller's obligation to erase personal data upon the data subject's request, the controller is obliged under the general principles of the GDPR to limit the personal data stored (see *Section 8*).

除控管者依當事人請求刪除個人資料之義務外，依GDPR的一般原則，控管者有義務限制所儲存之個人資料（見第8節）。

103. For video surveillance it is worth noticing that by for instance blurring the picture with no retroactive ability to recover the personal data that the picture previously contained, the personal data are considered erased in accordance with GDPR.

對於影像監控，值得注意的是，若以模糊化等方式處理圖像，且無法回復該圖像曾經含有的個人資料，則所含有的個人資料視為已經依GDPR刪除。

- 104.

Example: A convenience store is having trouble with vandalism in particular on its exterior and is therefore using video surveillance outside of their entrance in direct connection to the walls. A passer-by requests to have his personal data erased from that very moment. The controller is obliged to respond to the request without undue delay and at the latest within one month. Since the footage in question does no longer meet the purpose for which it was initially stored (no vandalism occurred during the time the data subject passed by), there is at the time of the request, no legitimate interest to store the data that would override the interests of the data subjects. The controller needs to erase the personal data.

示例：一家便利商店經常遭受故意破壞行為困擾，特別是對其外觀的破壞，並因此在其入口處與外牆連結處使用影像監控。一名路人請求刪除其經過時的個人資料。控管者有義務回應此請求，不得無故遲延，且至遲於一個月內回應。由於該影片已不再符合其最初儲存之目的（當事人經過時，並未發生破壞行為），在請求之時，儲

存該資料並無超越當事人權利的正當利益。控管者需要刪除該個人資料。

6.2.2 Right to object

拒絕權

105. For video surveillance based on *legitimate interest* (Article 6 (1) (f) GDPR) or for the necessity when carrying out a task in the *public interest* (Article 6 (1) (e) GDPR) the data subject has the right – at any time – to object, on grounds relating to his or her particular situation, to the processing in accordance with Article 21 GDPR. Unless the controller demonstrates compelling legitimate grounds that overrides the rights and interests of the data subject, the processing of data of the individual who objected must then stop. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month.

對於基於正當利益（GDPR第6條第1項第f款），或為執行符合公共利益之職務所必要（GDPR第6條第1項第e款）實施之影像監控，當事人依GDPR第21條，根據其個別狀況，有權利—隨時—拒絕該運用。除非控管者證明存在超越當事人權利和利益之必要正當理由，否則必須停止運用該拒絕者的資料。控管者有義務回應當事人之請求，不得無故遲延，且至遲於一個月內回應。

106. In the context of video surveillance this objection could be made either when entering, during the time in, or after leaving, the monitored area. In practice this means that unless the controller has compelling legitimate grounds, monitoring an area where natural persons could be identified is only lawful if either

影像監控的情況下，在進入該受監控區域、位於該區域內或離開該區域後，均可拒絕。實務中，這意味著除非控管者有必要正當理由，對自然人可被識別的特定區域實施監控，僅有在下列情況下合法：

(1) the controller is able to immediately stop the camera from processing personal data when requested, or

控管者能夠一經請求立即停止攝影機運用個人資料，或

(2) the monitored area is in such detail restricted so that the controller can assure the approval from the data subject prior to

entering the area and it is not an area that the data subject as a citizen is entitled to access.

受監控區域受嚴格限制，控管者能夠確保在各當事人進入該區域前獲得其同意，且該區域並非當事人作為公民有權進入之場所。

107. These guidelines do not aim to identify what is considered a compelling legitimate interest (Article 21 GDPR).

本指引無意釐清何者構成必要正當利益（GDPR第21條）。

108. When using video surveillance for direct marketing purposes, the data subject has the right to object to the processing on a discretionary basis as the right to object is absolute in that context (Article 21 (2) and (3) GDPR).

為行銷目的使用影像監控時，由於此時拒絕權係一絕對權利，當事人有權自主決定拒絕其運用（GDPR第21條第2項和第3項）。

109.

Example: A company is experiencing difficulties with security breaches in their public entrance and is using video surveillance on the grounds of legitimate interest, with the purpose to catch those unlawfully entering. A visitor objects to the processing of his or her data through the video surveillance system on grounds relating to his or her particular situation. The company however in this case rejects the request with the explanation that the footage stored is needed due to an ongoing internal investigation, thereby having compelling legitimate grounds to continue processing the personal data.

示例：一家公司正遭受其公共入口處保全問題困擾，並基於正當利益，為偵測非法進入者目的，運用影像監控。一名來訪者基於其個別狀況，拒絕以影像監控系統運用其資料。然而，該公司拒絕其請求，並解釋其進行中的內部調查需要儲存該影片，因此其有必要正當理由繼續運用該個人資料。

7 TRANSPARENCY AND INFORMATION OBLIGATIONS¹⁸

透明化和資訊提供義務¹⁸

110. It has long been inherent in European data protection law that data subjects should be aware of the fact that video surveillance is in operation. They should be informed in a detailed manner as to the places monitored.¹⁹ Under the GDPR the general transparency and information obligations are set out in Article 12 GDPR and following. Article 29 Working Party's "Guidelines on transparency under Regulation 2016/679 (WP260)" which were endorsed by the EDPB on May 25th 2018 provide further details. In line with WP260 par. 26, it is Article 13 GDPR, which is applicable if personal data are collected "[...] from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras [...])."

歐洲資料保護法向來要求應使當事人知曉影像監控正在運作，還應向其詳細告知受監控的地點¹⁹。依GDPR規定，一般透明化和資訊提供義務規定於GDPR第12條以下。EDPB於2018年5月25日採認之第29條工作小組（WP29）「關於第2016/679號規則（GDPR）中的透明化之指引（WP260）」包含更多的細節。依WP260第26段，若個人資料係「……以觀察方式（例如使用攝影機等自動化資料拍攝裝置或資料拍攝軟體）從當事人……」蒐集而得，則適用GDPR第13條。

111. In light of the volume of information, which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency (WP260, par. 35; WP89, par. 22). Regarding video surveillance the most important information should be displayed on the warning sign itself (first layer) while the further mandatory details may be provided by other means (second layer).

根據應向當事人提供之資訊的量，資料控管者得採用層級化方式，選擇使用不同方法之組合，以確保透明化（WP260，第35段；WP89，第22段）。關於影像監控，最重要的資訊應在警示標誌上顯示（第

¹⁸ Specific requirements in national legislation might apply.

可能適用國家立法中的特定要求。

¹⁹ See WP89, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance by Article 29 Working Party).

見WP89，第29條工作小組「關於以影像監控方式運用個人資料的意見4/2004」。

一層），而其他強制告知之資訊得以其他方式提供（第二層）。

7.1 First layer information (warning sign)

第一層資訊（警示標誌）

112. The first layer concerns the primary way in which the controller first engages with the data subject. At this stage, controllers may use a warning sign showing the relevant information. The displayed information may be provided in combination with an icon in order to give, in an easily visible, intelligible and clearly readable manner, a meaningful overview of the intended processing (Article 12 (7) GDPR). The format of the information should be adjusted to the individual location (WP89 par. 22).

第一層係關於控管者與當事人初始互動之主要方式。此一階段，控管者得使用警示標誌展示相關資訊。所展示的資訊得附有圖標，以便以易見、易懂且清晰易讀之方式，就預計之運用提出有意義之概述（GDPR第12條第7項）。應根據具體位置調整資訊之格式（WP89，第22段）。

7.1.1 Positioning of the warning sign

警示標誌之放置方式

113. The information should be positioned in such a way that the data subject can easily recognize the circumstances of the surveillance before entering the monitored area (approximately at eye level). It is not necessary to reveal the position of the camera as long as there is no doubt as to which areas are subject to monitoring and the context of surveillance is clarified unambiguously (WP 89, par. 22). The data subject must be able to estimate which area is captured by a camera so that he or she is able to avoid surveillance or adapt his or her behaviour if necessary.

資訊的放置方式應使得當事人能夠在進入受監控區域前，很容易地瞭解監控狀況（大約平視位置）。在清楚標示受監控之區域且確實說明監控狀況的前提下，不必指明攝影機的位置（WP89，第22段）。當事人必須能夠估測攝影機所拍攝的範圍，以便在必要時避開監控或調整其行為。

7.1.2 Content of the first layer

第一層內容

114. The first layer information (warning sign) should generally convey the most important information, e.g. the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impacts of the processing.²⁰ This can include for example the legitimate interests pursued by the controller (or by a third party) and contact details of the data protection officer (if applicable). It also has to refer to the more detailed second layer of information and where and how to find it.

第一層資訊（警示標誌）一般應傳達最重要的資訊，例如運用之目的、控管者身分和當事人權利等方面的細節，以及運用最為重要的影響²⁰。這可能包括，例如，控管者（或第三方）所追求的正當利益和個資保護長的聯絡資訊（若適用）。還應提及第二層更詳細的資訊，並說明在何處以何種方式獲得該資訊。

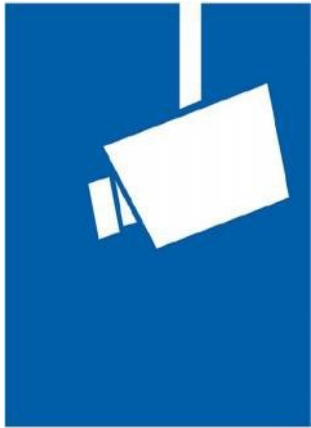
115. In addition the sign should also contain any information that could surprise the data subject (WP260, par. 38). That could for example be transmissions to third parties, particularly if they are located outside the EU, and the storage period. If this information is not indicated, the data subject should be able to trust that there is solely a live monitoring (without any data recording or transmission to third parties).

此外，該標誌還應包括可能使當事人感到意外的其他任何資訊（WP260，第38段）。這可能包括，例如，向第三方傳輸，特別是當該第三方位於歐盟境外時，以及儲存期間。若未說明這些資訊，當事人應能夠信任僅有單純的即時監控（不攝錄或向第三方傳輸任何資料）。

²⁰ See WP260, par. 38.
見WP260，第38段。

116.

Example:



Video surveillance!


Identity of the controller and, where applicable, of the controller's representative:

Contact details of the data protection officer (where applicable):

Purposes of the processing for which the personal data are intended as well as the legal basis for the processing:

Data subjects rights: As a data subject you have several rights against the controller, in particular the right to request from the controller access to or erasure of your personal data.

 For details on this video surveillance including your rights, see the full information provided by the controller through the options presented on the left.



Further information is available:

- via notice
- at our reception/ customer information/ register
- via internet (URL)...

示例：



錄影監控中！

控管者身分以及可適用的控管者代表：

個資保護長之聯絡資訊（如適用）：

個人資料預計運用之目的及其法律依據：

當事人權利： 作為當事人，您可對控管者行使數項權利，特別是向控管者請求存取資料或刪除您的個人資料。
 關於本影像監控之詳細資訊，包括您的權利，請見控管者透過左側所列選項提供之完整資訊。



更多資訊請見：

- 通知
- 我們的接待櫃檯/服務台/收銀櫃檯
- 網路（連結）……

7.2 Second layer information

第二層資訊

117. The second layer information must also be made available at a place easily accessible to the data subject, for example as a complete information sheet available at a central location (e.g. information desk, reception or cashier) or displayed on an easy accessible poster. As mentioned above, the first layer warning sign has to refer clearly to the second layer information. In addition, it is best if the first layer information refers to a digital source (e.g. QR-code or a website address) of the second layer. However, the information should also be easily available non-digitally. It should be possible to access the second layer information without entering the surveyed area, especially if the information is provided digitally (this can be achieved for example by a link). Other appropriate means could be a phone number that can be called. However the information is provided, it must contain all that is mandatory under Article 13 GDPR.

第二層資訊也必須在當事人易於獲取的位置提供，例如，可在某一核心位置（例如服務台、接待櫃檯或收銀櫃檯）提供完整資訊頁，或在易於參閱的海報上顯示。如前所述，第一層警示標誌必須明確提及第二層資訊。此外，最佳情況是，第一層資訊說明第二層資訊的數位資源（例如QR-code或網站網址）。然而，該資訊還應易於以非數位化方式獲取。第二層資訊應能在不進入受監控區域的情況下獲取，尤其是在該資訊以數位方式提供（例如，可透過連結而達成）。其他適當方式可以是能夠撥打的電話號碼。無論該資訊以何種方式提供，其必須包含GDPR第13條強制要求提供的全部資訊。

118. In addition to these options, and also to make them more effective, the EDPB promotes the use of technological means to provide information to data subjects. This may include for instance; geolocating cameras and including information in mapping apps or websites so that individuals can easily, on the one hand, identify and specify the video sources related to the exercise of their rights, and on the other hand, obtain more detailed information on the processing operation.

這些選項之外，同時也是為了增強這些選項的有效性，EDPB鼓勵使用技術方式向當事人提供資訊。這可能包括，例如，地理攝影機，在地圖繪製應用程式或網站中納入該資訊，以便個人能夠一方面輕

易地識別和明確行使其權利的相關影片來源，另一方面獲知關於運用作業的更詳細的資訊。

119.

Example: A shop owner is monitoring his shop. To comply with Article 13 it is sufficient to place a warning sign at an easy visible point at the entrance of his shop, which contains the first layer information. In addition, he has to provide an information sheet containing the second layer information at the cashier or any other central and easy accessible location in his shop.

示例：一名店主對其商店進行監控。為符合第13條，得在商店入口處顯著位置放置包含第一層資訊的警示標誌。此外，其還必須在收銀櫃檯或店內其他核心且易接近之位置提供包含第二層資訊的資訊頁。

8 STORAGE PERIODS AND OBLIGATION TO ERASURE

儲存期間和刪除義務

120. Personal data may not be stored longer than what is necessary for the purposes for which the personal data is processed (Article 5 (1) (c) and (e) GDPR). In some Member States, there may be specific provisions for storage periods with regards to video surveillance in accordance with Article 6 (2) GDPR.

個人資料的儲存期限不得超過其運用目的所必要的期間（GDPR第5條第1項第c款和第e款）。某些會員國可能依GDPR第6條第2項，對於影像監控的儲存期間有具體規定。

121. Whether the personal data is necessary to store or not should be controlled within a narrow timeline. In general, legitimate purposes for video surveillance are often property protection or preservation of evidence. Usually damages that occurred can be recognized within one or two days. To facilitate the demonstration of compliance with the data protection framework it is in the controller's interest to make organisational arrangements in advance (e. g. nominate, if necessary, a representative for screening and securing video material). Taking into consideration the principles of Article 5 (1) (c) and (e) GDPR, namely data minimization and storage limitation, the personal data should in most cases (e.g. for the purpose of detecting vandalism) be erased, ideally automatically, after a few days. The longer the storage period set (especially when beyond 72 hours), the more argumentation for the legitimacy of the purpose and the necessity of storage has to be provided. If the controller uses video surveillance not only for monitoring its premises but also intends to store the data, the controller must assure that the storage is actually necessary in order to achieve the purpose. If so, the storage period needs to be clearly defined and individually set for each particular purpose. It is the controller's responsibility to define the retention period in accordance with the principles of necessity and proportionality and to demonstrate compliance with the provisions of the GDPR.

個人資料的儲存必要性應控制於嚴格時限內。一般而言，影像監控的正當目的通常係保護財產或保存證據。所發生的損害通常能於一或兩天內發現。為協助證明符合資料保護體系，控管者宜事先進行

組織性安排（例如，在必要時指派代表過濾影片並對影片採取安全措施）。考量GDPR第5條第1項第c款和第e款規定之原則，亦即資料最小化和儲存限制，個人資料在大部分情況下（例如，為發現故意破壞行為）都應在數天後予以刪除（自動刪除更佳）。所設定的儲存期間越長（特別是若超過72小時），越需要論證目的正當性和儲存必要性。若控管者不僅使用影像監控其處所，還想要儲存該資料，則其必須確保儲存行為確實為實現其目的所必要。若是如此，則需為各項目的，分別明確定義其儲存期間。控管者有責任依必要性原則和比例原則定義保存期間，並證明遵守GDPR之規定。

122.

Example: An owner of a small shop would normally take notice of any vandalism the same day. In consequence, a regular storage period of 24 hours is sufficient. Closed weekends or longer holidays might however be reasons for a longer storage period. If a damage is detected he may also need to store the video footage a longer period in order to take legal action against the offender.

示例：一家小店的店主通常在破壞事故發生的當天即會注意到故意破壞行為。因此，一般儲存期間為24小時已經足夠。然而，週末或長假期間的店休可能是較長儲存期間的理由。若發現損害，其可能還需要將影片儲存較長期間，以便對行為人採取法律行動。

9 TECHNICAL AND ORGANISATIONAL MEASURES

技術性和組織性措施

123. As stated in Article 32 (1) GDPR, processing of personal data during video surveillance must not only be legally permissible but controllers and processors must also adequately secure it. Implemented **organizational and technical measures** must be **proportional to the risks to rights and freedoms of natural persons**, resulting from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to video surveillance data. According to Article 24 and 25 GDPR, controllers need to implement technical and organisational measures also in order to safeguard all data-protection principles during processing, and to establish means for data subjects to exercise their rights as defined in Articles 15-22 GDPR. Data controllers should adopt internal framework and policies that ensure this implementation both at the time of the determination of the means for processing and at the time of the processing itself, including the performance of data protection impact assessments when needed.

如GDPR第32條第1項所述，在影像監控期間運用個人資料不僅須為法律所允許，控管者和受託運用者還必須適當且充分地保護其安全。所實施的**組織性和技術性措施**，必須與所造成的**自然人的權利與自由之風險符合比例**，該風險可能係意外或違法破壞、丟失、竄改、未經授權揭露或存取影像監控資料而造成。依GDPR第24條和第25條，控管者還需執行技術性和組織性措施，以便在運用期間確保遵守一切資料保護原則，以及為了確立當事人行使GDPR第15條至第22條規定的各項權利的方法。資料控管者須採用內部體系和政策，以便在決定運用方法以及實際運用時可執行該等措施，包括必要時辦理個人資料保護影響評估。

9.1 Overview of video surveillance system

影像監控系統概述

124. A video surveillance system (VSS)²¹ consists of analogue and digital devices as well as software for the purpose of capturing images of a scene, handling the images and displaying them to an operator. Its components are grouped into the following categories:

影像監控系統（VSS）²¹包括類比和數位裝置及軟體，用以拍攝場景畫面、處理畫面並顯示予作業人員。其要素可分為如下兩類：

- Video environment: image capture, interconnections and image handling:

影像環境：畫面拍攝、互聯（interconnection）和畫面處理：

- the purpose of image capture is the generation of an image of the real world in such format that it can be used by the rest of the system,
拍攝畫面的目的係以系統其他部分可使用之格式，生成真實世界的影像；
- interconnections describe all transmission of data within the video environment, i.e. connections and communications. Examples of connections are cables, digital networks, and wireless transmissions. Communications describe all video and control data signals, which could be digital or analogue,
互聯描述影像環境內部的一切資料傳輸，亦即串聯（connection）和通訊（communication）。串聯的示例如線纜、數位網路和無線網路傳輸。通訊描述一切影片和控制資料訊號，可能係數位或類比性質。
- image handling includes analysis, storage and presentation of an image or a sequence of images.
畫面處理包括分析、儲存和呈現一幀畫面或一序列畫面。

- From the system management perspective, a VSS has the following logical functions:

系統管理方面，影像監控系統有下列邏輯功能：

- data management and activity management, which includes handling operator commands and system generated activities (alarm procedures, alerting operators),
資料管理和活動管理，包括處理作業人員命令和系統生成活動（警報程序、提醒作業人員）；

²¹ GDPR does not provide a definition for it, a technical description can for example be found in EN 62676-1- 1:2014 Video surveillance systems for use in security applications – Part 1-1: Video system requirements.

GDPR並未對此作定義，相關技術描述之示例為EN 62676-1- 1:2014，安全應用中使用之影像監控系統，第1-1部分，影像系統要求。

- interfaces to other systems might include connection to other security (access control, fire alarm) and non-security systems (building management systems, automatic license plate recognition).

對其他系統的介面可能包括連接至其他安全系統（權限控制、火災警報）和非安全系統（建築管理系統、自動車牌辨識）。

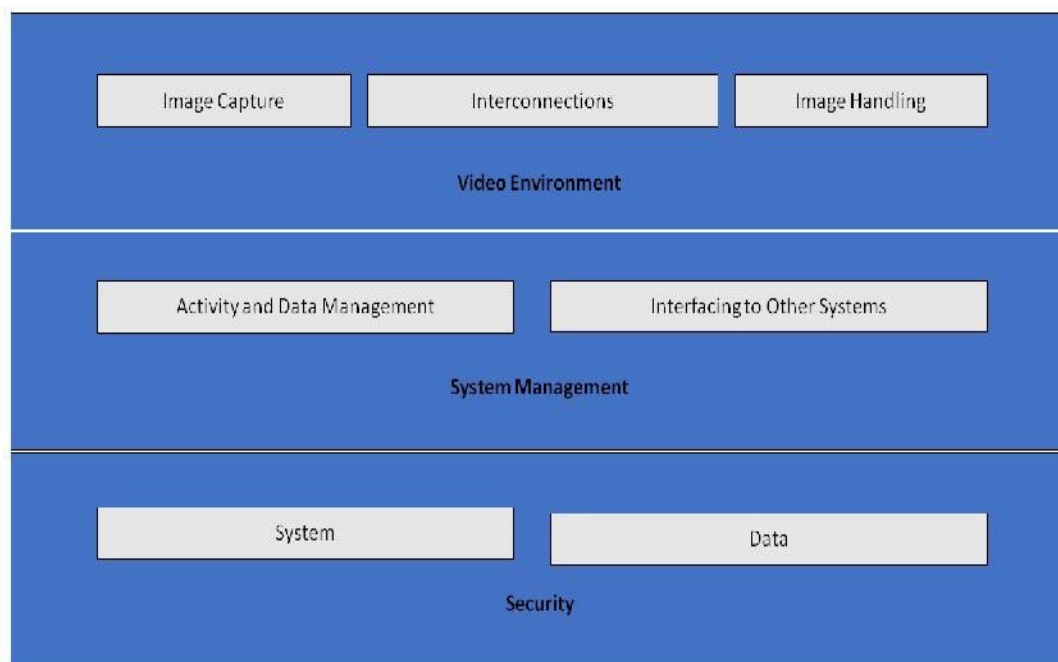
- VSS security consists of system and data confidentiality, integrity and availability:

影像監控系統安全包括系統和資料機密性、完整性和可用性：

- system security includes physical security of all system components and control of access to the VSS,
系統安全包括一切系統要素的實體安全（physical security）和該影像監控系統的權限控制；
- data security includes prevention of loss or manipulation of data.

資料安全包括防範資料丟失和竄改。

125.



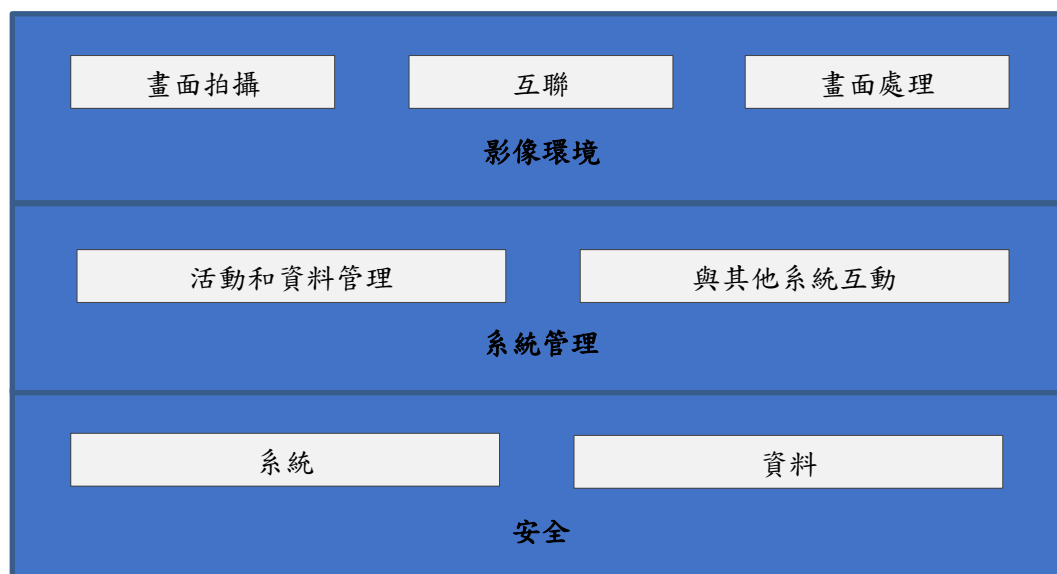


Figure 1- video surveillance system

圖1—影像監控系統

9.2 Data protection by design and by default

資料保護之設計和預設

126. As stated in Article 25 GDPR, controllers need to implement appropriate data protection technical and organisational measures as soon as they plan for video surveillance – before they start the collection and processing of video footage. These principles emphasize the need for built-in privacy enhancing technologies, default settings that minimise the data processing, and the provision of the necessary tools that enable the highest possible protection of personal data²².

如GDPR第25條所規定，控管者從開始計劃影像監控之時—在其開始蒐集和運用影片之前，就需要執行適當的技術性和組織性的資料保護措施。這些原則強調，需要內建式的隱私強化技術，最小化資料運用的預設設定以及提供必要工具，以實現最高程度的個資保護²²。

²² WP 168, Opinion on the "The Future of Privacy", joint contribution by the Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (adopted on 01 December 2009).

WP168，關於「隱私的未來」之意見，第29條個資保護工作小組和警察和司法工作小組對與歐盟執委會「關於個資保護基本權利的法律框架的諮商」之聯合提案（2009年12月1日通過）。

127. Controllers should build data protection and privacy safeguards not only into the design specifications of the technology but also into organisational practices. When it comes to organisational practices, the controller should adopt an appropriate management framework, establish and enforce policies and procedures related to video surveillance. From the technical point of view, system specification and design should include requirements for processing personal data in accordance with principles stated in Article 5 GDPR (lawfulness of processing, purpose and data limitation, data minimisation by default in the sense of Article 25 (2) GDPR, integrity and confidentiality, accountability etc.). In case a controller plans to acquire a commercial video surveillance system, the controller needs to include these requirements in the purchase specification. The controller needs to ensure compliance with these requirements applying them to all components of the system and to all data processed by it, during their entire lifecycle.

控管者在技術的設計規格方面，以及組織性實務方面，皆應建立資料保護和隱私安全維護措施。在組織性實務方面，控管者應採行適當的管理體系，確立並實施影像監控相關之政策和程序。從技術的角度，系統規格和設計應包括依GDPR第5條規定的原則運用個人資料之要求（運用之合法性、目的和資料限制、GDPR第25條第2項意義上的預設資料最小化、完整性和機密性、課責性等）。若控管者計劃購買商業影像監控系統，則需要在訂單規格中納入這些要求。控管者需要確保遵守這些要求，並在其運作之完整期間內，將其適用於系統的全部要素及其所運用的全部資料。

9.3 Concrete examples of relevant measures

相關措施的具體示例

128. Most of the measures that can be used to secure video surveillance, especially when digital equipment and software are used, will not differ from those used in other IT systems. However, regardless of the solution selected, the controller must adequately protect all components of a video surveillance system and data under all stages, i.e. during storage (data at rest), transmission (data in transit) and processing (data in use). For this, it is necessary that controllers and processors combine organisational and technical measures.

大部分可用於確保影像監控安全的措施，特別是所使用的數位設備和軟體，與其他IT技術系統所使用的並無不同。然而，無論選擇何種方案，控管者都必須充分保護影像監控系統的全部要素和各階段資料，亦即，儲存階段（靜止資料）、傳輸階段（傳輸中的資料）和運用階段（使用中的資料）。為此，控管者和受託運用者有必要結合組織性和技術性的措施。

129. When selecting technical solutions, the controller should consider privacy-friendly technologies also because they enhance security. Examples of such technologies are systems that allow masking or scrambling areas that are not relevant for the surveillance, or the editing out of images of third persons, when providing video footage to data subjects.²³ On the other hand, the selected solutions should not provide functions that are not necessary (e.g., unlimited movement of cameras, zoom capability, radio transmission, analysis and audio recordings). Functions provided, but not necessary, must be deactivated.

選擇技術方案時，控管者還應考慮隱私友好的技術，因為其能增強安全性。這種技術的示例係，在向當事人提供影片時，能夠遮蔽或加擾與監控無關之區域、或將第三人的影像編輯移除的系統²³。另一方面，所選擇的方案不應提供非必要功能（例如，攝影機不受限制的移動、變焦能力、無線電傳輸、分析和錄音）。所提供的非必要功能必須予以關閉。

130. There is a lot of literature available on this subject, including international standards and technical specifications on the physical security of multimedia systems²⁴, and the security of general IT systems²⁵. Therefore, this section provides only a high-level overview of this topic.

此一主題有許多文獻，包括多媒體系統實體安全²⁴與一般IT技術系統安全²⁵相關的國際標準和技術規格。因此，本節僅對此一主題進行簡

²³ The use of such technologies may even be mandatory in some cases in order to comply with Article 5 (1) (c). In any case they can serve as best practice examples.

某些情況下，為符合第5條第1項第c款，甚至強制使用這些技術。無論如何，其可作為最佳實務之示例。

²⁴ IEC TS 62045 — Multimedia security - Guideline for privacy protection of equipment and systems in and out of use.

IEC TS 62045—多媒體安全—關於使用中和已停用的設備和系統之隱私保護指引。

²⁵ ISO/IEC 27000 — Information security management systems series

要回顧。

9.3.1 Organisational measures

組織性措施

131. Apart from a potential DPIA needed (see *Section 10*), controllers should consider the following topics when they create their own video surveillance policies and procedures:

除可能需要個資保護影響評估（DPIA）外（見第10節），控管者在構建其影像監控政策和程序時，還應考慮下列問題：

- Who is responsible for management and operation of the video surveillance system.
何人負責管理和運作該影像監控系統。
- Purpose and scope of the video surveillance project.
該影像監控計畫的目的和範圍。
- Appropriate and prohibited use (where and when video surveillance is allowed and where and when it is not; e.g. use of hidden cameras and audio in addition to video recording)²⁶.
適當的和被禁止的使用（何時何地允許使用影像監控，何時何地不得使用；例如，使用隱藏式攝影機、錄影同時錄音）²⁶。
- Transparency measures as referred to in *Section 7 (Transparency and information obligations)*.
第7節（透明化和資訊提供義務）所述之透明化措施。
- How video is recorded and for what duration, including archival storage of video recordings related to security incidents.
錄影的方法及其時限，包括將安全事故相關的錄影建檔儲存。
- Who must undergo relevant training and when.
何人必須於何時接受相關培訓。
- Who has access to video recordings and for what purposes.
何人得為哪些目的存取影片。
- Operational procedures (e.g. by whom and from where video surveillance is monitored, what to do in case of a data breach

ISO/IEC 27000—資訊安全管理系統系列。

²⁶ This may depend on national laws and sector regulations.
可能依國內法和行業規則而不同

incident).

作業程序（例如，何人於何地觀看監控畫面，發生資料侵害事故時如何因應）。

- What procedures external parties need to follow in order to request video recordings, and procedures for denying or granting such requests.

外部人員如請求提供影片，應遵守哪些程序，拒絕或同意此等請求之程序。

- Procedures for VSS procurement, installation and maintenance.

影像監控系統採購、安裝和維護程序。

- Incident management and recovery procedures.

事故管理和恢復程序。

9.3.2 Technical measures

技術性措施

132. **System security** means **physical security** of all system components, and system integrity i.e. **protection against and resilience under intentional and unintentional interference with its normal operations and access control**. Data security means **confidentiality** (data is accessible only to those who are granted access), **integrity** (prevention against data loss or manipulation) and **availability** (data can be accessed when it is required). 系統安全係指一切系統要素的實體安全與系統完整性，亦即，防範和因應對其正常作業與存取權限控制的有意或無意干擾。資料安全係指機密性（只有經授權者可存取資料），完整性（防止資料丟失或竄改）和可用性（在需要時可存取資料）。

133. **Physical security** is a vital part of data protection and the first line of defence, because it protect VSS equipment from theft, vandalism, natural disaster, manmade catastrophes and accidental damage (e.g. from electrical surges, extreme temperatures and spilled coffee). In case of an analogue based systems, physical security plays the main role in their protection.

實體安全是資料保護的重要部分且為第一道防線，其保護影像監控系統設備免受竊盜、故意破壞、自然災害、人為災禍和意外損害（例如，突波、極端溫度和打翻的咖啡）。在類比系統中，實體安全是主要保護措施。

134. **System and data security**, i.e. protection against intentional and unintentional interference with its normal operations may include:

系統和資料安全（亦即，防範對其正常作業的有意或無意干擾）可能包括：

- Protection of the entire VSS infrastructure (including remote cameras, cabling and power supply) against physical tampering and theft.
保護影像監控系統基礎設施之整體（包括遠端攝影機、線纜和電源）免受實體破壞和竊取。
- Protection of footage transmission with communication channels secure against interception
以安全通訊通道傳輸影片，防範攔截。
- Data encryption.
資料加密。
- Use of hardware and software based solutions such as firewalls, antivirus or intrusion detection systems against cyber attacks.
使用防火牆、防毒和入侵偵測系統等軟硬體解決方案，防範網路攻擊。
- Detection of failures of components, software and interconnections.
偵測元件、軟體和互聯故障。
- Means to restore availability and access to the system in the event of a physical or technical incident.
發生實體或技術事故時，恢復可用性和系統可存取性的方法。

135. **Access control** ensures that only authorized people can access the system and data, while others are prevented from doing it. Measures that support physical and logical access control include:

存取權限控制確保只有經授權者才能存取系統和資料，防止他人存取。支援實體和邏輯存取控制的措施包括：

- Ensuring that all premises where monitoring by video surveillance is done and where video footage is stored are secured against unsupervised access by third parties.
確保受影像監控和儲存影片的一切場所皆採取安全措施，防範第三方在未經監督的情況下闖入。

- Positioning monitors in such a way (especially when they are in open areas, like a reception) so that only authorized operators can view them.
調整顯示器位置（特別是當其位於接待櫃檯等開放區域時），使其僅能由授權作業人員觀看。
- Procedures for granting, changing and revoking physical and logical access are defined and enforced.
定義並實施授予、變更和撤銷實體和邏輯存取權限的程序。
- Methods and means of user authentication and authorization including e.g. passwords length and change frequency are implemented.
使用者認證和授權的方式與方法，包括實施密碼長度和修改頻率要求等。
- User performed actions (both to the system and data) are recorded and regularly reviewed.
記錄並定期審查使用者（對系統和對資料）實施之行動。
- Monitoring and detection of access failures is done continuously and identified weaknesses are addressed as soon as possible.
持續監控和偵測存取失敗，識別並儘快修正弱點。

10 DATA PROTECTION IMPACT ASSESSMENT

個資保護影響評估

136. According to Article 35 (1) GDPR controllers are required to conduct data protection impact assessments (DPIA) when a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons. Article 35 (3) (c) GDPR stipulates that controllers are required to carry out data protection impact assessments if the processing constitutes a systematic monitoring of a publicly accessible area on a large scale. Moreover, according to Article 35 (3) (b) GDPR a data protection impact assessment is also required when the controller intends to process special categories of data on a large scale.

根據GDPR第35條第1項，若某種資料運用可能導致對自然人權利與自由的高風險，控管者須辦理個資保護影響評估。GDPR第35條第3項第c款規定，若運用構成對公眾開放區域之大規模系統性監控，須辦理個資保護影響評估。此外，GDPR第35條第3項第b款規定，若控管者有意大規模運用特種個資，亦須辦理個資保護影響評估。

137. The Guidelines on Data Protection Impact Assessment²⁷ provide further advice, and more detailed examples relevant to video surveillance (e.g. concerning the “use of a camera system to monitor driving behaviour on highways”). Article 35 (4) GDPR requires that each supervisory authority publish a list of the kind of processing operations that are subject to mandatory DPIA within their country. These lists can usually be found on the authorities’ websites. Given the typical purposes of video surveillance (protection of people and property, detection, prevention and control of offences, collection of evidence and biometric identification of suspects), it is reasonable to assume that many cases of video surveillance will require a DPIA. Therefore, data controllers should carefully consult these documents in order to determine whether such an assessment is required and conduct it if necessary. The outcome of the performed DPIA should determine the controller’s choice of implemented data protection measures.

「關於個資保護影響評估之指引」²⁷對影像監控提供進一步建議與更

²⁷ WP248 rev.01, 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. - endorsed by the EDPB

詳細的示例（例如「使用攝影系統監控高速公路上的駕駛行為」）。GDPR第35條第4項要求各監管機關公布該國境內強制辦理DPIA之運用作業清單。這些清單通常刊載於機關網站上。考量到影像監控的典型目的（保護人員與財產，偵測、防範和控制違法行為，蒐集證據和嫌犯生物特徵），可合理假設很多影像監控將需要辦理個資保護影響評估。因此，資料控管者應仔細參閱這些文件，以確定是否應辦理評估，並在必要時辦理評估。所辦理的個資保護影響評估之結果應決定控管者選擇執行之資料保護措施。

138. It is also important to note that if the results of the DPIA indicate that processing would result in a high risk despite security measures planned by the controller, then it will be necessary to consult the relevant supervisory authority prior to the processing. Details on prior consultations can be found in Article 36.

還應注意，若個資保護影響評估結果顯示，雖有控管者計劃採取的安全措施，運用仍可能造成高風險，則有必要在運用前諮詢相關監管機關。此等事前諮詢的詳細資訊見於第36條。

For the European Data Protection Board

The Chair

(Andrea Jelinek)

歐盟個人資料保護委員會
主席

(Andrea Jelinek)

WP248 rev.01，關於第 2016/679號規則（GDPR）中的個資保護影響評估（DPIA）以及確認運用是否「可能造成高風險」之指引，EDPB採認。

GDPR 相關指引文件研析/葉奇鑫計畫主持 -- 初版 --

臺北市：國發會，民 109.09

面：表，公分

編號：(109)020.0904

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

資訊法規

312.07

GDPR 相關指引文件研析

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

計畫主持人：葉奇鑫

出版機關：國家發展委員會

電話：02-23165300

地址：臺北市寶慶路 3 號

網址：<http://www.ndc.gov.tw/>

出版年月：中華民國 109 年 9 月

版次：初版

刷次：第 1 刷

編號：(109)020.0904 (平裝)