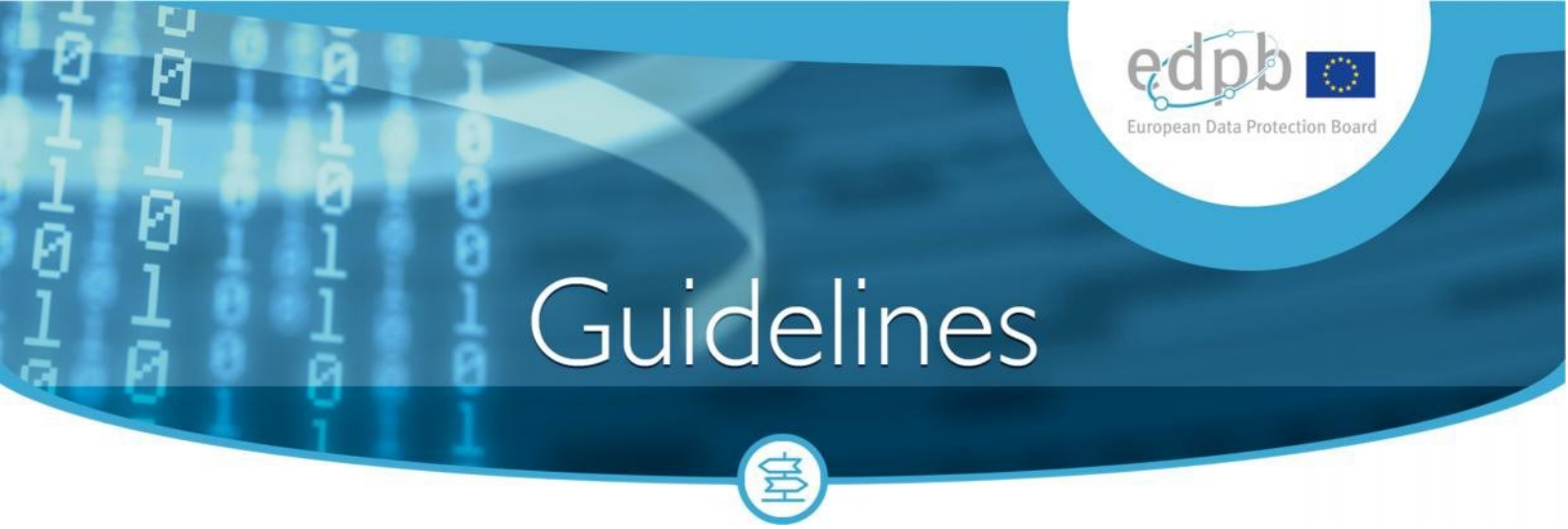

Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak

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

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[1],

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[1]；

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，個資保護在建構信任、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 virus[2].

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 data[4] 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 users[5].
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 consent[6] 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 objectives[7].

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 exist[9], 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 shown[10] 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-conscientious 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 controllers[11] 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 Members 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) GDPR[14] or for health care purposes as described in Art. 9(2)(h) GDPR[15]. 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 Default[17], 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 approach[18]. 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.

為保護伺服器和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**	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. 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。 Parameters for duration of exposure and distance

	between people must be estimated by the health authorities and can be set in the application. 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。
Location data **位置資料**	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: 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： • 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***	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.

	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。
Virus carrier **病毒帶原者**	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. 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。
Contact tracing **接觸史追蹤**	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. 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。 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. 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。

3. General

總則

GEN-1	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 only up until the point manual contact tracing techniques can manage alone the amount of new infections. 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，即應停止使用該應用程式。
GEN-2	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). 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。
GEN-3	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. 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

	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	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. 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。

4. Purposes

目的

PUR-1	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. 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。
PUR-2	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. 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。
PUR-3	The application must not be used to draw conclusions on the

	location of the users based on their interaction and/or any other means. 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。

5. Functional considerations

功能性考量

FUNC-1	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). 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）。
FUNC-2	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. 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。
FUNC-3	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

	knowledge on the spread of the virus. 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。
FUNC-4	**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. **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。
FUNC-5	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. 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。

6. Data
資料

DATA-1	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. 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。
DATA-2	This broadcast data must include cryptographically strong pseudo-random identifiers, generated by and specific to the application.

	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。
DATA-3	The risk of collision between pseudo-random identifiers should be sufficiently low. 隨機假名識別碼間的重複機率應足夠低。
DATA-4	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. 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。
DATA-5	According to the data minimisation principle, the application must not collect data other than what is strictly necessary for the purpose of contact tracing 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。
DATA-6	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. 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

	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	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. 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。
DATA-8	Users must be informed of all personal data that will be collected. This data should be collected only with the user authorization. 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。

7. Technical properties
技術屬性

TECH-1	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. 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。
TECH-2	The application should keep the history of a user's contacts in the equipment, for a predefined limited period of time. 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。

TECH-3	The application may rely on a central server to implement some of its functionalities. 應用程式得透過中央伺服器執行部分功能。
TECH-4	The application must be based on an architecture relying as much as possible on users' devices. 應用程式之基礎架構必須儘可能地依賴使用者的裝置。
TECH-5	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. 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。

8. Security
安全

SEC-1	A mechanism must verify the status of users who report as SARS-CoV-2positive 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. 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。
SEC-2	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.

	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。
SEC-3	Requests must not be vulnerable to tampering by a malicious user 不得讓惡意使用者輕易竄改請求。
SEC-4	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. 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。
SEC-5	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. 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。

SEC-6	In order to avoid impersonation or the creation of fake users, the server must authenticate the application. 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。
SEC-7	The application must authenticate the central server. 應用程式必須對中央伺服器進行認證。
SEC-8	The server functionalities should be protected from replay attacks. 應保護伺服器功能免受重送攻擊（replay attack）。
SEC-9	The information transmitted by the central server must be signed in order to authenticate its origin and integrity. 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。
SEC-10	Access to all data stored in the central server and not publicly available must be restricted to authorised persons only. 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。
SEC-11	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. 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。

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	A Data Protection Impact Assessment must be carried out and should be made public. 須辦理個資保護影響評估並公開其結果。
PRIV-7	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. 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。
PRIV-8	The information conveyed by the application must not allow users to identify users carrying the virus, nor their movements. 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。
PRIV-9	The information conveyed by the application must not allow health authorities to identify potentially exposed users without their agreement. 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。
PRIV-10	Requests made by the applications to the central server must not reveal anything about the virus carrier. 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。
PRIV-11	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. 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

	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 *non-colluding servers 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*（*non-colluding servers*）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

	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. 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。

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 declined[19] 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」。

	on their part. 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。
CON-2	The central server must not maintain nor circulate a list of the pseudonymous identifiers of users carrying the virus. 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。
CON-3	Contact history stored on the central server must be deleted once users are notified of their proximity with a positively diagnosed person. 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。
CON-4	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. 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。
CON-5	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). 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）。
CON-6	Contact histories submitted by distinct users should not further be processed e.g. cross-correlated to build global proximity maps. 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。

CON-7	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。

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	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. 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。
ID-2	The central server must not maintain nor circulate the contact history of users carrying the virus. 中央伺服器不得保存或傳播病毒帶原者的接觸史記錄。
ID-3	Identifiers stored on the central server must be deleted once they were distributed to the other applications. 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。
ID-4	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. 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。

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。