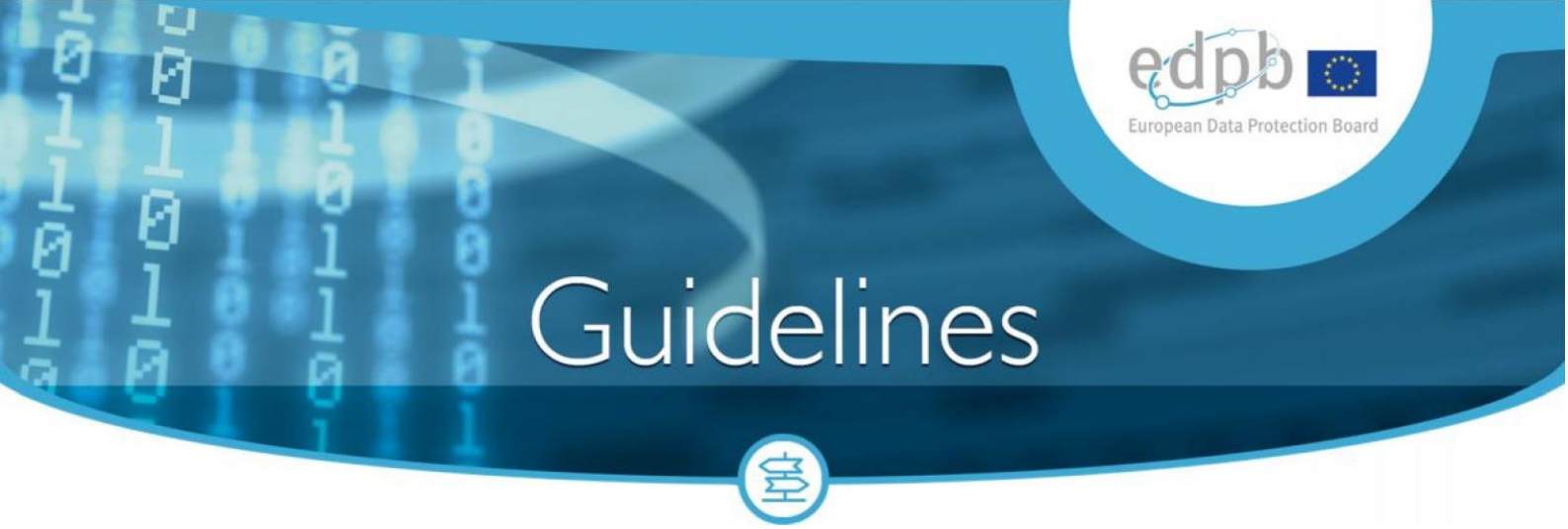

Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak

COVID-19 発生に関連した位置情報および接触追跡ツールの使用に関するガイドライン 04/2020

（参考訳）

Adopted on 21 April 2020

2020 年 4 月 21 日採択

Table of contents

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,
欧州データ保護委員会は
個人データの処理および当該データの自由な移動に関する自然人の保護に関する 2016 年 4 月 27 日の欧州議会および理事会規則 2016/679/EU の第 70 条(1)項(e)を考慮し、指令 95/46/EC（以下「GDPR」）を廃止し、
2018 年 7 月 6 日の EEA 合同委員会決定第 154/2018 号により改正された EEA 協定、特にその附属書 XI 及び議定書 37 を考慮し、
第 12 条及び第 22 条の手続規則を尊重し、

HAS ADOPTED THE FOLLOWING GUIDELINES:
以下のガイドラインを採用する。

1 INTRODUCTION & CONTEXT
1 イントロダクションとコンテキスト

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.

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.

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.

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.

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

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

- 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 ;
- 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.

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.

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].

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]

1 政府や民間企業は、COVID-19 パンデミックへの対応の一環として、データを活用したソリューションの利用に目を向けており、多くのプライバシー問題が提起されている。

2 EDPB は、データ保護の法的枠組みは柔軟に設計されており、パンデミックを抑制する効率的な対応と基本的人権と自由の保護の両方を達成することができることを強調している。

3 EDPB は、COVID-19 パンデミックを管理するために個人データの処理が必要な場合、信頼を築き、いかなる解決策であれそれが社会的に受け入れられる条件を作り、それによってこれらの対策の有効性を保証するためには、データ保護が不可欠であると確信している。ウイルスに国境はないのだから、現在の危機に対応するためには、欧州で共通のアプローチを開発するか、少なくとも相互運用可能な枠組みを整備することが望ましいと考えられる。

4 EDPB は一般的に、COVID-19 対策に使用されるデータや技術は、個人をコントロールしたり、汚名を着せたり、抑圧したりするためではなく、個人を力づけるために使用されるべきであると考えている。さらに、データと技術は重要なツールになり得るが、それらには本質的な限界があり、他の公衆衛生対策の有効性を一層活用するものに過ぎない。有効性、必要性、比例性の一般原則は、COVID-19 対策のための個人データの処理を伴う加盟国や EU の機関が採用するあらゆる対策の指針とならなければならない。

5 本ガイドラインは、特に以下の 2 つの目的のために位置情報と接触追跡ツールを比例的に使用するための条件と原則とを明確にしている。

- 位置情報を使用して、ウイルスの拡散をモデル化してパンデミックへの対応を支援し、封じ込め対策の全体的な有効性を評価すること。

- 接触追跡によって、汚染の連鎖をできるだけ早く断ち切るために、最終的にウイルスのキャリアであることが確認された人の近くにいたという事実を個人に通知すること。

6 接触追跡アプリケーションがパンデミックの管理に貢献する効率性は、多くの要因（例えば、インストールを必要とする人の割合、近接性と期間の点での「接触」の定義など）に依存する。さらに、このようなアプリケーションは、パンデミックと戦うための包括的な公衆衛生戦略の一部である必要があり、このような包括的な戦略には、特に、疑念を取り除くための検査およびこれに続く手動による接触追跡が含まれる。このようなアプリケーションの導入には、ユーザーに提供される情報が文脈に沿ったものであること、および警告が公衆衛生システムに有用であることを保証するための支援策を伴うべきである。そうでなければ、これらのアプリケーションの効果が十分に発揮されない可能性がある。

7 EDPB は、GDPR と指令 2002/58/EC（「ePrivacy Directive」）の両方には、SARS-CoV-2 ウイルス の拡散を監視し、封じ込めるために、国や EU レベルで公的機関やその他の関係者を支援するための匿名または個人データの使用を認める特定の規則が含まれていることを強調している。

8 この点に関して、EDPB は、接触追跡アプリケーションの使用は任意であるべきであり、個人の動きの追跡ではなく、利用者に関する近接情報に依拠すべきであるという事実について、すでに見解を示している。

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

[33] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 USE OF LOCATION DATA
2 位置情報の利用

2.1 Sources of location data
2. 1 位置情報のソース

9 There are two principal sources of location data available for modelling the spread of the virus and the overall effectiveness of confinement measures:

- location data collected by electronic communication service providers (such as mobile telecommunication operators) in the course of the provision of their service ; and
- location data collected by information society service providers' applications whose functionality requires the use of such data (e.g., navigation, transportation services, etc.).

10 The EDPB recalls that location data[2] 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[3].

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[4] or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the user.

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[5].

13 As for the re-use of location data collected by an information society service provider for modelling purposes (e.g., through the operating 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.[6]

9 ウイルスの拡散と封じ込め対策の全体的な有効性をモデル化するために利用できる位置情報源は、主に 2 つある。

- 電子通信サービス提供者（移動体通信事業者など）がサービスを提供する過程で収集した位置情報；および

- 情報社会サービス提供者のアプリケーションが収集した位置情報データであって、アプリケーションの機能がそのようなデータの使用を必要とするもの（例：ナビゲーション、交通サービスなど）。

[2] See Art. 2(c) of the ePrivacy Directive.
[3] See Art 6 and 9 of the ePrivacy Directive.
[4] 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
[5] 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.
[6] See section 1.5.3 of the guidelines 1/2020 on processing personal data in the context of connected vehicles.

10 EDPB は、電子通信事業者から収集された位置情報は、ePrivacy 指令の第 6 条と第 9 条の範囲内でのみ処理が許されることに注意を促す。つまり、これらのデータは、プロバイダによって匿名化されている場合、またはトラフィックデータではない利用者の端末機器の地理的位置を示すデータについては、利用者の事前の同意を得た場合に限り、当局またはその他の第三者に送信することができるということである。

11 端末機器から直接収集される位置情報を含む情報については、ePrivacy 指令の第 5 条(3)項が適用される。したがって、利用者の端末に情報を保存したり、既に保存されている情報にアクセスしたりすることは、(i)利用者の同意がある場合、または(ii)利用者が明示的に要求した情報社会サービスのために厳格に必要な場合に限って認められる。

12 しかし、「ePrivacy」指令に規定されている権利及び義務に関する例外は、第 15 条に従って可能である。すなわち、民主主義社会の中で特定の目的のために必要かつ適切かつ比例した措置となる場合には例外となり得る。

13 情報社会サービス提供者がモデリング目的で収集した位置情報を再利用する場合（例えば、オペレーティングシステムや以前にインストールされていたアプリケーションを介して再利用する場合)、追加の条件を満たさなければならない。実際、データが ePrivacy 指令の第 5 条(3)項に準拠して収集された場合は、データの再利用には追加の条件を満たさなければならない。ePrivacy 指令の第 5 条(3)に従ってデータが収集された場合には、データ主体の追加的な同意がある場合、または第 23 条(1)で言及されている目的を守るために民主主義社会において必要かつ比例した措置を構成する連合または加盟国の法律に基づいてのみ、データはさらに処理することができる。

2.2 Focus on the use of anonymised location data

2. 2 匿名化された位置情報の利用について

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.

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

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).

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.

18 Many options for effective anonymisation exist[7], 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

[7] (de Montjoye et al., 2018) "On the privacy-conscientious use of mobile phone data”

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.

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.

20 Indeed, a large body of research has shown[8][9] 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.

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 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.

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.

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

14 EDPB は、位置情報を使用する場合は、個人情報ではなく、匿名化されたデータの処理を優先すべきであることを強調する。

15 匿名化とは、いかなる「合理的な」努力をしても、データを識別され、または識別され得る自然人と結びつけることができなくなるよう、一連の技術を用いることである。この「合理性のテスト」においては、客観的な側面（時間、技術的手段）と、個別事案ごとに異なる状況に関する要素（人口密度、データの性質、量などの現象の希少性）の両方を考慮しなければならない。もしデータがこのテストに合格しない場合、そのデータは匿名化されていないことになり、GDPR の適用範囲内に留まることになる。

16 匿名化の堅牢性の評価は、以下の 3 つの基準に基づいている。匿名化の堅牢性を評価するには、次の 3 つの基準が必要である：(i) singling-out（データに基づいて個人をより大きなグループの中で探し出せるかどうか）、(ii) linkability（同じ個人に関する 2 つの記録をリンクさせることができるかどうか）、(iii) inference（個人に関する未知の情報を有意な確率で推論することができるかどうか）。

17 匿名化の概念は誤解されやすく、仮名化と誤解されることが多い。匿名化はデータを制限なく使用することを可能にするが、仮名化されたデータは依然として GDPR の適用範囲内にある。

18 効果的な匿名化のための多くの選択肢が存在するが、注意点がある。データはそれ自体を匿名化することはできない。つまり、データセット全体について匿名化することができたり、匿名化することができなかったりする。この意味では、暗号化その他の数学的変換など

[8] (de Montjoye et al., 2013) "Unique in the Crowd: The privacy bounds of human mobility" and (Pyrgelis et al.,
[9]) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data"

による単一のデータパターンに基づくいかなる操作も、せいぜい仮名化としか考えられない。

19 匿名化プロセスと再識別攻撃は活発な研究分野である。匿名化ソリューションを実装している管理者は、この分野の最近の動向を監視することが非常に重要であり、特に匿名化が困難であることが知られている（通信事業者や 情報社会サービスに由来する）位置情報に関するデータについては特に注意が必要である。

20 実際、匿名化されていると思われていた位置情報が、実際には匿名化されていない可能性があることが多くの研究で示されている。個人の移動の痕跡は本質的に非常に相関性が高く、固有のものである。そのため、特定の状況下では、再識別の試みに対して脆弱である可能性がある。

21 長期間にわたって個人の位置を追跡した単一のデータパターンを完全に匿名化することはできない。記録された地理的座標の精度が十分に低下させられていない場合や、追跡の詳細が削除され、データ対象者が長期間滞在する場所の位置のみが 保持されている場合であっても、完全には匿名化し得ないというこの評価はなお変わらない可能性がある。これは、集約化が不十分な位置情報についても同様である。

22 匿名化を実現するためには、位置情報データは合理性テストを満たすために慎重に処理されなければならない。この意味で、このような処理には、位置情報データセット全体を考慮することと、利用可能な堅牢な匿名化技術が適切かつ効果的に実装されていることを条件に、合理的な程度に大規模な個人群からのデータを処理することが含まれる。

23 最後に、匿名化処理の複雑さを考慮すると、匿名化方法についての透明性を高めることが強く推奨される。

3 CONTACT TRACING APPLICATIONS
3 接触追跡アプリケーション

3.1 General legal analysis
3. 1 一般的な法的分析

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.

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[10] 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.

[10] 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. [12] See Recital (41).

26 In addition, with regard to the principle of purpose limitation, the purposes must be specific enough to exclude further processing for purposes unrelated to the management of the COVID19 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.

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:

- contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used;
- as contact tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification;
- the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.

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.

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.

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]

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.

32 However, if the data processing is based on another legal basis, such as consent (Art. 6(1)(a))[11]for example, the controller will have to ensure that the strict requirements for such legal basis to be valid are met.

33 Moreover, the use of an application to fight the COVID-19 pandemic might lead to the

[11] 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.
[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.

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[12]. Depending on the legal basis, it might also be based on explicit consent (Art. 9(2)(a) GDPR).

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.

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.

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.

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.

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.

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)[13]. The EDPB strongly recommends the publication of DPIAs.

24 自然人の位置情報や人との接触を系統的かつ大規模に監視することは、そのプライバシーに対する重大な侵入である。 このような処理は、利用者が、関連する各目的のために自発的に受け入れることに依拠することによってのみ正当化され得る。このことは、特に、そのようなアプリケーションを使用しないと決めた、または使用できない個人がいかなる不利益をも被るべきではないことを意味する。

25 説明責任を確保するために、接触追跡アプリケーションの管理者は明確に定義されるべきである。EDPB は、国の保健当局がそのようなアプリケーションの管理者となりうると考えるが、それ以外の管理者も想定しうる。いずれの場合においても、接触追跡アプリの展開に異なる主体が関与する場合には、その役割と責任が最初から明確に定義され、利用者に説

[12] See Article 9(2)(h) GDPR

[13] 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. [17] See EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

明されなければならない。
26 さらに、目的に照らした処理限定の原則の観点から、COVID19 による健康危機への対処とは無関係な目的（商業目的や法執行目的など）のための追加的な処理を排除しうる程度に目的が十分具体的でなければならない。ひとたび目的が明確に定義された後は、個人データの使用が（そのような目的に照らして）適切で、必要で、かつ比例したものであることを確保する必要がある。
27 接触追跡アプリケーションを利用する状況においては、データの最小化と、設計及び初期設定によるデータ保護の原則に対して慎重な考慮が払われるべきである。すなわち、
- 接触追跡アプリは、個々のユーザーの位置を追跡する必要はなく、人同士の接近に関するデータを使用すべきである。
- 接触追跡アプリは、個人を直接識別することなく機能し得るので、再識別を防ぐための適切な措置を講じるべきである。
- 収集された情報は利用者の端末機器に留まるべきであり、絶対的に必要な場合にのみ関連する情報を収集すべきである。
28 処理の適法性に関して、接触追跡アプリケーションは端末装置への情報の保存および（または）端末装置に既に保存されている情報への アクセスを伴うものであり、ePrivacy 指令第 5 条(3)項の適用対象となることを EDPB は指摘する。アプリケーションの提供者がユーザーから明示的に要求されたサービスを提供するためにこれらの操作が厳格に必要な場合、これらの処理についてユーザーの同意は必要ない。厳格に必要ではない操作については、提供者は利用者の同意を求める必要がある。
29 さらに、接触追跡アプリケーションの利用が自発的に行われるという事実だけでは、個人データの処理が必ずしも 同意に基づいて行われることを意味しないと EDPB は指摘する。公的機関が法により与えられた権限に基づき、法が定める要件に従ってサービスを提供する場合においては、そのような処理について最も関連性のある法的根拠は、GDPR 第 6 条(1)(e)、すなわち「公共の利益に関わる業務を遂行するための必要性」であると思われる。
30 GDPR 第 6 条(3)では、第 6 条(1)(e)で言及されている処理の根拠は、EU 法または管理者が服する加盟国国内法によって規定されていなければならないと明示されている。処理の目的は、その法的根拠に基づいて決定されるか、または第 6 条(1)(e)で言及された処理に関しては、公共の利益に関わる業務の遂行もしくは管理者に与えられた公的権限の行使に関わる業務の執行のために必要とされるものでなければならない。
31 しかし、接触追跡アプリケーション使用の適法根拠を提供する法的根拠または立法措置は、例えばアプリケーション利用の任意性に言及するなど、意味のあるデータ保護措置を組み込んでいるべきである。（そのような法的根拠または立法措置には、）個人データの追加的利用に関する明確な目的の特定と明示的な制限が含まれ、関係する管理者が誰であるかが明確に定義されていなければならない。また、データのカテゴリー、および個人データが開示

される可能性のある主体（およびその目的）も特定されていなければならない。プライバシーへの干渉の程度に応じて、処理の性質、範囲、目的を考慮して、追加の保護措置が組み込まれるべきである。最後に、可能な限り速やかに、アプリケーションをいつ廃止するかを決定するための基準と、そのような決定を行うための権限と説明責任を持つのは誰であるかを（これらの法的根拠または立法措置には）含めることを EDPB は推奨する。

33 さらに、COVID-19 パンデミックと戦うためにアプリケーションの使用が健康データ（例えば感染者の状態）の収集につながる場合がある。このようなデータの処理が許容される場合として、公衆衛生の分野における公共の利益のために必要であって GDPR14 の第 9 条(2)(i)項の条件を満たす場合、または、第 9 条(2)(h)に規定される医療・健康管理の目的のために必要な場合がある。適法根拠としては、明示的な同意に基づく場合もある（GDPR 第 9 条(2)(a)）。

34 当初の目的次第では、GDPR 第 9 条(2)(j)は、科学的研究の目的または統計的な目的のために必要な場合には、健康データを処理することも許容している。

35 現在の健康危機は、（目的に照らし）比例性を欠くデータ保持の権限を確立する機会として利用されてはならない。保持制限は、真の必要性および医学的関連性（これには潜伏期間などの疫学的な考慮が含まれる場合がある）を考慮すべきであり、個人データは COVID-19 危機の期間のみ保持されるべきである。その後は、原則として、すべての個人データは消去または匿名化されるべきである。

36 EDPB が理解するところ、このようなアプリは、資格のある公衆衛生担当者が行う手動による接触の追跡に取って代わるものではなく、これを支援するものに過ぎず、そのような担当者が濃厚接触がウイルス感染につながる可能性が高いかどうかを選別できる（例えば、レジ係など、適切な装備で保護された人と接した場合、感染の可能性があるかどうか）。EDPB は、接触者追跡アプリが実装する関連アルゴリズムを含む手順や処理は、誤検知の発生を抑制するために、有資格者の厳格な監督の下で動作すべきであることを強調する。特に、次に何をすべきかの助言を提供する作業は、自動化された処理のみに基づくものであってはならない。

37 公平性、説明責任、そしてより広くは法律の遵守を保証するために、アルゴリズムは監査可能でなければならず、 独立した専門家によって定期的にレビューされなければならない。アプリケーションのソースコードは、可能な限り広範な精査のために公開されなければならない。

38 誤検出は常にある程度の確率で発生する。感染リスクの特定は、検査が陰性になるまで自己隔離を続けるなど、個人に大きな影響を与える可能性があるため、データやその後の分析結果を修正することができることは必要不可欠である。もちろん、このことが当てはまるのは、データの処理及び／又は保存が技術的に可能であって、上記のような悪影響が発生する可能性が高いシナリオ及び実装においてのみである。

39 最後に、EDPB は、処理が高リスクである可能性が高いと考えられる（健康データ、予

想される大規模な採用、システマティックなモニタリング、新しい技術的ソリューションの使用）ため、そのようなツールを実施する前にデータ保護の影響評価（DPIA）を実施しなければならないと考える。EDPB は、DPIA 結果の公表を強く推奨する。

3.2 Recommendations and functional requirements
3. 2 推奨事項と機能要件

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.

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.

42 Implementations for contact tracing can follow a centralized or a decentralized approach[14]. 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 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.

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.

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.

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.

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.

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.

40 デザインによるデータ保護およびデフォルトによるデータ保護のさまざまな対策のうち、データ最小化の原則によれば、処理されるデータは厳密に最小化されなければならな

[14] In general, the decentralised solution is more in line with the minimisation principle

い。アプリケーションは、既婚・未婚、通信識別子、機器のディレクトリ項目、メッセージ、通話ログ、位置データ、機器の識別子などを含む、無関係な情報や必要のない情報を収集してはならない。

41 アプリケーションによってブロードキャストされるデータは、アプリケーションによって生成され、アプリケーションに固有の、いくつかのユニークな仮名の識別子のみに留めなければならない。これらの識別子は、定期的に更新されなければならず、ウイルスの拡散を抑制する目的と相容れる頻度で、個人の識別と物理的な追跡のリスクを制限するのに十分な頻度で更新されなければならない。

42 接触追跡のための実装には、中央集権的アプローチと分散型アプローチが考えられる。適切なセキュリティ対策が講じられていれば、どちらも実行可能な選択肢であると考えられるべきであり、それぞれには利点と欠点が伴う。したがって、アプリ開発の概念的な段階では、データ保護／プライバシーへのそれぞれの影響と個人の権利へ の影響を慎重に検討し、両方の概念を徹底的に検討することが常に含まれているべきである。

43 連絡先追跡システムに関与するサーバーは、保健当局による適切な評価とユーザーの自発的な行動の結果として、 感染したと診断されたユーザーの接触履歴または仮名化された識別子のみを収集しなければならない。あるいは、サーバーは、感染した可能性のあるユーザーに曝露を知らせるための期間のみ、感染したユーザーの仮名化された識別子のリストまたはその接触履歴を保持しなければならず、感染した可能性のあるユーザーを特定しようとしてはならない。

44 アプリケーションと手動によるトレースの両方を含む全体的な接触追跡方法を導入するには、場合によっては追加の情報処理を要する可能性がある。このような状況においては、この追加情報はユーザーの端末に残り、厳密に必要な場合にのみ、ユーザーの事前の、同意対象を明らかにした同意を得た上で処理されるべきである。

45 サーバーやアプリケーションに格納されたデータ、アプリケーションとリモートサーバー間のデータ交換を安全にするために、最先端の暗号化技術を実装しなければならない。アプリケーションとサーバー間の相互認証も行われなければならない。

46 アプリケーション上での COVID-19 に感染したユーザーの報告は、例えば、感染者の仮名の ID に結び付けられ、検査ステーションや医療専門家にリンクされた、1 回限り使用できるコードを介して、適切な承認を受けなければならない。安全な方法で確認を得ることができない場合は、ユーザーの状態に関する情報が信頼できるとの推定に基づくデータ処理を行ってはならない。

47 管理者は、個人が第三者のアプリを利用するリスクを軽減するために、公的機関と協力して、国の公式連絡先追跡アプリをダウンロードするためのリンクについて、明確かつ明示的に通知しなければならない。

4 CONCLUSION
4 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.

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.

48 世界は、強力な対応を必要とする重大な公衆衛生危機に直面しており、そのような対応はこの緊急事態を超えて影響を及ぼすことになる。自動化されたデータ処理とデジタル技術は、COVID-19 との戦いにおいて重要な要素となり得る。しかし、「ラチェット効果」には注意が必要である。このような異常な状況下で取られるすべての措置が必要であり、期間的に限定され、最小限の範囲であり、定期的かつ真正なレビューと科学的評価の対象となることを保証することは、我々の責任である。

49 EDPB は、現在の危機への効率的な対応と基本的権利の保護のどちらかを選択すべきではないことを強調している：私たちは両方を達成することができ、さらにデータ保護の原則は、ウイルスとの戦いにおいて非常に重要な役割を果たすことができる。欧州のデータ保護法は、健康管理の目的で個人データを、責任を持って使用することを認めており、その過程で個人の権利と自由が侵食されないようにしている。

For the European Data Protection Board
The Chair
(Andrea Jelinek)

ANNEX -- CONTACT TRACING APPLICATIONS ANALYSIS GUIDE
付録 -- 接触追跡アプリケーション分析ガイド

0. Disclaimer

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).

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.

0. 免責事項

以下のガイダンスは、規定的なものでも網羅的なものでもなく、本ガイドの唯一の目的は、コンタクトトレーシングアプリケーショ ンの設計者と実装者に一般的なガイダンスを提供することである。ここで説明したもの以外のソリューションを使用することができ、関連する法的枠組み(すなわち GDPR と ePrivacy 指令)に準拠している限り、合法的である。また、このガイドは一般的な性質のものであることにも留意しなければならない。したがって、本書に含まれる推奨事項や義務は、網羅的なものではない。評価はケースバイケースで行われなければならず、特定のアプリケーションでは、このガイドに含まれていない追加的な措置が必要となる場合がある。

1. Summary

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*.

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.

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.

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.

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

- 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.

- 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.

- 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.

- 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.

- 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:

    - 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.

    - 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.

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

    - 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).

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

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

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

- 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.

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.

1 まとめ

多くの加盟国の利害関係者は、SARS-Cov-2*に感染した人と接触したかどうかを住民が発見できるようにするために、接触追跡*アプリケーションの利用を検討している。

このようなアプリケーションがパンデミックへの対処に効果的に貢献する条件はまだ確立されていない。また、このようなアプリが導入される前に、これらの条件が確立されている必要がある。しかし、設計の初期段階から個人情報の保護が保証されるように、上流工程の開発チームに関連情報を提供するためのガイドラインを提供することは重要である。

このガイドは一般的な性質のものであることに注意しなければならない。したがって、本書に含まれる推奨事項や義務は、網羅的なものではないと見なすべきである。評価はケースバイケースで行われなければならず、特定のアプリケーションでは、このガイドに含まれていない追加の対策が必要になる場合がある。本ガイドの目的は、コンタクトトレースアプリケーションの設計者および実施者に一般的なガイダンスを提供することである。

いくつかの基準は、データ保護の枠組みに由来する厳格な要件を超えているかもしれない。これらの基準は、そのような接触追跡アプリが社会的に受け入れられるように、最高レベルの透明性を確保することを目的としている。

このため、コンタクトトレースアプリケーションの発行者は、以下の基準を考慮する必要がある。

- このようなアプリケーションの使用は、厳密に任意でなければならない。アプリの使用を法律で保証される権利行使の条件としてはならない。個人は常に自分のデータに対する完全な管理権を有しなければならず、そのようなアプリケーションを使用するかどうかを自由に選択できるようにしなければならない。
- 接触追跡アプリケーションは、自然人の権利と自由に対するリスクが高く、導入前にデータ保護の影響評価が必要となる可能性が高い。

- アプリケーションのユーザー間の近接性に関する情報は、ユーザーの位置を特定することなく得ることができる。この種のアプリケーションは、位置情報の使用を必要とせず、したがって、位置情報の使用を伴うべきではない。
- 利用者が SARS-Cov-2 ウイルスに感染していると診断された場合には、接触追跡のための疫学的に意味がある保持期間内に密接に接触した者のみに通知されるべきである。
- このタイプのアプリケーションの運用には、選択されたアーキテクチャによっては、集中型サーバーの使用が必要となる場合がある。このような場合、データの最小化と設計上のデータ保護の原則に従って、集中型サーバーで処理されるデータは最小限に制限されなければならない。
    - ユーザーが感染していると診断された場合、当該ユーザーの同意がある場合に限り、当該ユーザーのアプリからブロードキャストされる、当該ユーザーの以前の密接な接触者に関する情報または当該ユーザーの識別子を収集することができる。ユーザーを特定せずに、その人が本当に感染していることを主張できる検証方法を確立する必要がある。技術的には、例えば、特別なワンタイムコードを使用するなど、医療専門家の介入の後にのみ接触者に警告を発することで達成することができる。
    - 中央サーバーに保存された情報は、感染していると診断されたユーザーやそのユーザーと接触していた ユーザーを管理者が特定することを可能にしてはならず、また、関連する接触の判定に必要のない接触パターンの 推測を可能にしてはならない。
- この種のアプリケーションの動作には、他のユーザーのデバイスによって読み取られるようデータをブロードキャストしたり、そのようなブロードキャストを聞いたりする必要がある。
    - ユーザーのモバイル機器（コンピュータ、タブレット、接続された時計など）間で、例えばブロードキャスティング（例えば Bluetooth Low Energy 技術を介して）によって、仮名の識別子を交換することで十分である。
    - 識別子は、最先端の暗号化プロセスを用いて生成されなければならない。
    - 識別子は、物理的な追跡やリンケージ攻撃のリスクを軽減するために、定期的に更新する必要がある。

- このタイプのアプリケーションは、安全な技術プロセスを保証するために安全性が確保されていなければならない。特に
    - アプリケーションは、利用者が他人の身元や診断を推測できるような情報を利用者に伝えてはならない。中央サーバーは、利用者を特定したり、利用者に関する情報を推測したりしてはならない。

免責事項：上記の原則は、接触追跡アプリケーションの主張された目的に関連するものであり、ウイルスにさらされている可能性のある人々に（彼らを特定することなく）自動的に通知することのみを目的としたこの目的にのみ関連している。これらのガイドラインのすべてまたは一部に従うことは、データ保護の枠組みに完全に準拠するためには必ずしも十分ではない。

2. Definitions

2 . 定義

Contact 接触者	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. 接触者追跡アプリケーションでは、接触者とは、ウイルスのキャリアであることが確認されたユーザーとの交流に参加したユーザーであり、その持続時間と距離が、ウイルス感染への重大な曝露のリスクを誘発するものである。
	Parameters for duration of exposure and distance between people must be estimated by the health authorities and can be set in the application. 曝露時間と人と人との距離のパラメータは、保健当局によって推定されなければならず、アプリケーションで設定することができる。
Location data 位置データ	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: • the latitude, longitude or altitude of the terminal equipment; • the direction of travel of the user; or • the time the location information was recorded.

	これは、電子通信ネットワークまたは電子通信サービスで処理されるすべてのデータであって、公衆に利用可能な電子通信サービス（e-Privacy 指令で定義されている）の利用者の端末装置の地理的位置を示すもので、他の潜在的なソースからのデータと同様に、以下に関連している。 • 端末装置の緯度、経度又は高度。 • 利用者の進行方向 • 位置情報が記録された時間
Interaction 交流	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. コンタクトトレースアプリケーションの文脈において、交流とは、使用される通信技術（例：Bluetooth）の範囲内で、お互いに（空間的にも時間的にも）近接した位置にある 2 つのデバイス間の情報交換と定義される。この定義では、交流に関わる 2 人のユーザーの位置は除外される。
Virus carrier ウイルスキャリア	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. この文書では、ウイルスキャリアとは、ウイルス検査で陽性と判定され、医師や保健所から正式な診断を受けたユーザーを指すと考える。
Contact tracing 接触追跡	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. 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. （疫学者によって定義された基準に基づいて）ウイルスに感染した人と密接に接触した人は、感染し、他の人にも感染する大きなリスクがある。 接触追跡は、感染の危険性があるかどうかを確認し、適切な衛生措置を講じるために、ウイルス感染者の近くにいたすべての人をリストアップする疾病管理の方法である。

3. General

3. 一般

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. このアプリケーションは、従来の接触追跡技術（特に感染者へのインタビュー）を補完するツールでなければならず、より広範な公衆衛生プログラムの一部でなければならない。それは、手動の接触追跡技術だけでは新しい感染症の量を管理することができるポイントまでのみ使用されなければならない。
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). 遅くとも、管轄の公的機関が「正常な状態への復帰」を決定した場合には、識別子の収集を停止し（アプリケーションのグローバルな停止、アプリケーションのアンインストール指示、自動アンインストールなど)、すべてのデータベース（モバイルアプリケーションとサーバー）から収集したすべてのデータの削除を有効にするための手順を実施しなければならない。
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. アプリケーションのソースコードとそのバックエンドのソースコードはオープンでなければならず、技術仕様は公開されなければならない。 これにより、関係者がコードを監査し、必要に応じてコードの改善、可能性のあるバグの修正、個人データの処理の透明性の確保に貢献することができる。
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. アプリケーションの展開の段階では、公衆衛生の観点からアプリケーションの有効性を段階的に検証できるようにしなければならない。この目的のために、アプリケーションの有効性を測定するための指標を指定した評価手順を上流で定義しなければならない。

4. Purposes

4. 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. アプリケーションは、SARS-Cov-2 ウイルスに潜在的にさらされている人々に注意を喚起し、対処できるように、接触追跡の唯一の目的を追求しなければならない。アプリケーションを他の目的に使用してはならない。
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. アプリケーションは、検疫または監禁措置および/または社会的距離の遵守を監視する目的のための主たる用途から転用されてはならない。
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. アプリケーションは、ユーザーの交流および/またはその他の手段に基づくユーザーの位置に基づいて結論を導き出すために使用されてはならない。

5. Functional considerations

5. 機能的配慮

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). アプリケーションは、ウイルスに感染した可能性があることをユーザーに知らせる機能を提供しなければならない。この情報は、スクリーニング検査の陽性の前の X 日（X 値は保健当局によって定義されている）の期間内の感染したユーザーへの近接性に基づいている。
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. アプリケーションは、ウイルスに曝された可能性があると識別されたユーザーに勧告を提供しなければならない。それは、ユーザーが従うべき措置に関する指示を中継し、ユーザーが助言を要求できるようにしなければならない。このような場合には、人間の介入が必須となる。
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.

	距離と時間の要因を考慮に入れて感染リスクを測定するアルゴリズムは、接触者がいつ接触者追跡リストに記録されなければならないかを決定し、ウイルスの拡散に関する最新の知識を考慮に入れて安全に調整できるようにしなければならない。
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. ウイルスの潜伏期間内に、利用者は、ウイルスに感染した場合には情報を与えられ、または、ウイルスに感染したか否かの情報を定期的に入手しなければならない。
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. アプリケーションは、他の EU 加盟国で開発された他のアプリケーションとの相互運用性があり、異なる加盟国間を移動するユーザーに効率的に通知を行うことができるようにしなければならない。

6. Data

6. データ

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. アプリケーションは、接触の追跡を実行できるように、Bluetooth Low Energy のような近接通信技術を介してデータをブロードキャストしたり受信したりすることができる必要がある。
DATA-2	This broadcast data must include cryptographically strong pseudo-random identifiers, generated by and specific to the application. この放送データには、アプリケーションによって生成され、アプリケーションに固有の、暗号的に強力な擬似ランダム識別子が含まれていなければならない。
DATA-3	The risk of collision between pseudo-random identifiers should be sufficiently low. 疑似ランダム識別子同士が衝突するリスクは十分に低くなければならない。
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. 疑似ランダム識別子は、中央サーバーのオペレータ、他のアプリケーションのユーザー、悪意のある第三者を含むいかなる者による個人の再識別、物理的な追跡

	またはリンクのリスクを制限するのに十分な頻度で、定期的に更新されなければならない。これらの識別子は、中央サーバーから提供されたシードに基づいて、ユーザーのアプリケーションによって生成されなければならない。
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 データ最小化の原則に従い、アプリケーションは、接触追跡の目的のために厳密に必要なデータ以外のデータを収集してはならない。
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. アプリケーションは、接触追跡の目的で位置情報を収集してはならない。位置情報は、アプリケーションが他の国の類似アプリケーションと交流することを可能にするという唯一の目的のためにのみ処理することができ、この唯一の目的のために厳密に必要な精度に制限されなければならない。
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. 本アプリは、任意で、かつユーザーへの情報提供の意思決定を補助する目的により行う場合以外、本アプリの目的のために厳格に必要なもの以上に健康データを収集してはならない。
DATA-8	Users must be informed of all personal data that will be collected. This data should be collected only with the user authorization. ユーザーは、収集されるすべての個人データを知らされなければならない。このデータは、ユーザーの許可を得てのみ収集される。

7. Technical properties

7. 技術的特性

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. アプリケーションは、アプリケーションを実行しているデバイスの近傍にいるユーザーを検出するために、近接通信技術（例えば、Bluetooth Low Energy）を使用するなどの技術を利用できるようにする必要がある。
TECH-2	The application should keep the history of a user's contacts in the equipment, for a predefined limited period of time. アプリケーションは、ユーザーの接触履歴を、予め設定された限られた期間に限り装置内に保持すべきである。

TECH-3	The application may rely on a central server to implement some of its functionalities. アプリケーションは、その機能の一部を実装するために中央サーバーに依存してもよい。
TECH-4	The application must be based on an architecture relying as much as possible on users' devices. アプリケーションは、ユーザーのデバイスに可能な限りユーザーの装置に依存するアーキテクチャに基づいていなければならない。
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. ウイルス感染が報告された利用者の主導で、かつ、適切に認定された医療従事者が確認した後、利用者の接触履歴または利用者自身の識別子を中央サーバーに送信べきである。

8. Security

8. セキュリティ

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. SARS-CoV-2 陽性と報告したユーザーの状態を、例えば、テストステーションや医療従事者にリンクされた単一の使用コードの提供などにより検証するメカニズムがなければならない。安全な方法で確認できない場合は、データを処理してはならない。
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. 中央サーバーに送信されるデータは、安全なチャネルを介して送信されなければならない。OS プラットフォームプロバイダが提供する通知サービスの使用は慎重に評価されるべきであり、第三者へのデータ開示につながるものであってはならない。
SEC-3	Requests must not be vulnerable to tampering by a malicious user リクエストは、悪意のあるユーザーによる改ざんに対して脆弱であってはならない。

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. アプリケーションとサーバー間、およびアプリケーション間のやりとりを安全にするために、また、原則として、アプリケーションとサーバーに保存されている情報を保護するために、最先端の暗号技術を実装しなければならない。使用可能な技術の例としては、例えば、対称暗号化、非対称暗号化、ハッシュ関数、プライベートメンバーシップテスト、プライベート集合の交点、ブルームフィルタ、プライベート情報検索、同型暗号化などが挙げられる。
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. 中央サーバーは、積極的に診断を受けて接触履歴を送信した利用者や自身の識別子を含むいかなる利用者のネットワーク接続識別子（IP アドレスなど）も保持してはならない。
SEC-6	In order to avoid impersonation or the creation of fake users, the server must authenticate the application. なりすましや偽ユーザーの作成を避けるために、サーバーはアプリケーションを認証する必要がある。
SEC-7	The application must authenticate the central server. アプリケーションは中央サーバーを認証する必要がある。
SEC-8	The server functionalities should be protected from replay attacks. サーバー機能はリプレイ攻撃から保護されている必要がある。
SEC-9	The information transmitted by the central server must be signed in order to authenticate its origin and integrity. 中央サーバーから送信される情報は、その出所と完全性を認証するために署名されなければならない。
SEC-10	Access to all data stored in the central server and not publicly available must be restricted to authorised persons only. 中央サーバーに保存され、一般に公開されていないすべてのデータへのアクセスは、権限のある者のみに制限されなければならない。

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. オペレーティングシステムレベルでのデバイスのパーミッションマネージャは、通信モジュールにアクセスして必要なときに使用したり、端末にデータを保存したり、中央サーバーと情報を交換したりするために必要なパーミッションのみを要求しなければならない。

9. Protection of personal data and privacy of natural persons *Reminder: the following guidelines concern an application whose sole purpose is contact tracing.*

9. 個人データと自然人のプライバシーの保護 注意：以下のガイドラインは、接触の追跡を唯一の目的とするアプリケーションに関するものである。

PRIV-1	Data exchanges must be respectful of the users' privacy (and notably respect the principle of data minimisation). データ交換は、利用者のプライバシーを尊重しなければならない（特にデータ最小化の原則を尊重しなければならない)。
PRIV-2	The application must not allow users to be directly identified when using the application. アプリケーションを使用する際には、ユーザーを直接特定できないようにしなければならない。
PRIV-3	The application must not allow users' movements to be traced. アプリケーションは、ユーザーの動きをトレースできるようにしてはならない。
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). アプリケーションの使用により、ユーザーが他のユーザーについて何も知ることができないようにすべきである（とくにウイルスキャリアであるかどうか)。
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. 中央サーバーへの信頼は限定的でなければならない。中央サーバーの管理は、明確に定義された統治規則に従うとともに、そのセキュリティを確保するために 必要なすべての措置を含めなければならない。中央サーバーの所在場所は、所轄の監督当局による効果的な監督が可能になるようにしなければならない。
PRIV-6	A Data Protection Impact Assessment must be carried out and should be made public. データ保護影響評価を実施し、公表する必要がある。

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. アプリケーションは、ウイルスに曝露されたかどうかだけをユーザーに明らかにし、可能であれば、他のユーザーの情報や曝露された回数と日付を明らかにしてはならない。
PRIV-8	The information conveyed by the application must not allow users to identify users carrying the virus, nor their movements. アプリケーションから伝達される情報により、ウイルスを所持しているユーザーを特定したり、その動きを特定したりすることができないようにしなければならない。
PRIV-9	The information conveyed by the application must not allow health authorities to identify potentially exposed users without their agreement. アプリケーションによって伝達される情報によって、保健当局は、本人の同意なしに、潜在的に露出しているユーザーを特定することができないようにしなければならない。
PRIV-10	Requests made by the applications to the central server must not reveal anything about the virus carrier. アプリケーションから中央サーバーへのリクエストは、ウイルスキャリアについて何も明らかにしてはならない。
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. アプリケーションから中央サーバーへの要求は、必要な場合のみ仮名の識別子と連絡先リストを明らかにする場合を除き、ユーザーに関する不必要な情報を明らかにしてはならない。
PRIV-12	Linkage attacks must not be possible. リンケージ攻撃は可能であってはならない。
PRIV-13	Users must be able to exercise their rights via the application. 利用者は、アプリケーションを介して権利を行使することができなければならない。
PRIV-14	Deletion of the application must result in the deletion of all locally collected data. アプリケーションを削除すると、ローカルに収集されたすべてのデータが削除されなければならない。

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. アプリケーションは、他の同アプリケーションまたは相互運用可能な同等のアプリケーションによって送信されたデータのみを収集しなければならない。他のアプリケーション及び／又は近接通信装置に関するデータを収集してはならない。
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. 中央サーバーによる再識別を避けるために、プロキシサーバーを実装すべきである。これらの非共謀サーバーの目的は、中央サーバーと共有する前に、複数のユーザーの識別子(ウイルスキャリアの識別子とリクエスターによって送られた識別子の両方)を混合し、中央サーバーがユーザーの識別子(IP アドレスなど)を知ることを防ぐことである。
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. アプリケーションとサーバーは、不要なデータを収集しないように（例えば、サーバーのログに識別子を含めないなど)、また他の目的のためにデータを収集するサードパーティの SDK を使用しないように、慎重に開発・設定しなければならない。

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 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.

現在議論されているほとんどの接触者追跡アプリケーションは、ユーザーが感染していると宣言されたときに、基本的に 2 つのアプローチに従う：スキャンによって得られた近接接触者の履歴をサーバーに送信するか、またはブロードキャストされた自身の識別子のリストをサーバーに送信するかである。以下の原則は、これらの 2 つのアプローチに従って否定される。これら２つのアプローチがここで議論されているが、それは他のアプローチ、例えば、何らかの形でＥ2Ｅ（エンドトゥーエンド）暗号化を実装したり、あるいは他のセキュリテ

ィまたはプライバシーを強化する技術を適用するアプローチが不可能であるとか、ましてや望ましいということを意味しない。

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

9.1. アプリケーションが接触者のリストをサーバーに送信する場合にのみ適用される原則

CON-1	The central server must collect the contact history of users reported as positive to COVID-19 as a result of voluntary action on their part. 中央サーバーは、ユーザー側の自発的な行動の結果でなければ、COVID-19 陽性であると報告されたユーザーの接触履歴を収集してはならない。
CON-2	The central server must not maintain nor circulate a list of the pseudonymous identifiers of users carrying the virus. 中央サーバーは、ユーザー側の自発的な行動の結果でなければ、COVID-19 陽性であると報告されたユーザーの接触履歴を収集してはならない。
CON-3	Contact history stored on the central server must be deleted once users are notified of their proximity with a positively diagnosed person. セントラルサーバーに保存されている連絡履歴は、陽性と診断された人との接近を利用者に通知された時点で削除する必要がある。
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. 陽性と判定されたユーザーが中央サーバーとの接触履歴を共有する場合や、ユーザーがサーバーにウイルスにさらされている可能性を調べるためのリクエストを行う場合を除いて、ユーザーの機器からデータを持ち出すことはできない。
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). ローカルヒストリーに含まれるすべての識別子は、その収集から X 日後に削除されなければならない（X 値は保健当局によって定義される）。
CON-6	Contact histories submitted by distinct users should not further be processed e.g. cross-correlated to build global proximity maps. あるユーザーが送信した接触履歴を追加的に処理してはならない。例えば、全体的な接触マップを作成するために関連付けるなどの処理をしてはならない。
CON-7	Data in server logs must be minimised and must comply with data protection requirements

	サーバーログのデータは最小限に抑え、データ保護の要件に準拠しなければならない。

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

9.2. アプリケーションが自身の識別子のリストをサーバーに送信する場合にのみ適用される原則

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. 中央サーバーは、COVID-19 陽性であると報告されたユーザーのアプリケーションによってブロードキャストされた識別子を、ユーザー側の自発的な行動の結果として収集しなければならない。
ID-2	The central server must not maintain nor circulate the contact history of users carrying the virus. 中央サーバーは、ウイルスを保有しているユーザーの接触履歴を維持したり、回覧したりしてはならない。
ID-3	Identifiers stored on the central server must be deleted once they were distributed to the other applications. 中央サーバーに保存されている識別子は、他のアプリケーションに配布された後に削除する必要がある。
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. 陽性であると検出されたユーザーが中央サーバーと識別子を共有する場合を除き、データはユーザーの機器から離れてはならないし、ユーザーがウイルスにさらされている可能性を調べるためにサーバーにリクエストを行った場合、データはユーザーの機器から離れてはならない。
ID-5	Data in server logs must be minimised and must comply with data protection requirements サーバーログのデータは最小限に抑え、データ保護の要件に準拠しなければならない。