Насоки № 4/2020 относно използването на данни за местонахождение и инструменти за проследяване на контакти в контекста на пандемията от COVID-19

Приети на 21 април 2020 г.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Приет документ

История на версиите

Версия 1.1	5 май 2020 г.	Незначителни поправки
Версия 1.0	21 април 2020 г.	Приемане на Насоките

Съдържание

Европейският комитет по защита на данните,

като взе предвид член 70, параграф 1, буква д) от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за ЕИП, и по-специално приложение XI и Протокол 37 от него, изменени с Решение № 154/2018 на Съвместния комитет на ЕИП от 6 юли 2018 г.[1],

като взе предвид членове 12 и 22 от Процедурния си правилник,

ПРИЕ СЛЕДНИТЕ НАСОКИ:

1 ВЪВЕДЕНИЕ И КОНТЕКСТ

1 Правителствата и частните субекти се насочват към използването на основани на данните решения като част от отговора на пандемията от COVID-19, което поражда многобройни опасения във връзка с неприкосновеността на личния живот.

2 Европейският комитет по защита на данните (наричан по-нататък „ЕКЗД“) подчертава, че правната уредба за защита на данните е проектирана така, че да е гъвкава и поради това е в състояние да осигури както ефикасна реакция за ограничаване на пандемията, така и защита на правата на човека и основните свободи.

3 ЕКЗД категорично вярва, че когато обработването на лични данни е необходимо за справянето с пандемията от COVID-19, защитата на данните е наложителна, за да се изгради доверие у хората и да се създадат условия за социалната приемливост на дадено решение, с което съответно да се гарантират и ефективността на тези мерки. Тъй като вирусът не признава граници, изглежда е за предпочитане да се разработи общ европейски подход в отговор на настоящата криза или поне да се въведе оперативно съвместима рамка.

4 ЕКЗД принципно счита, че използваните данни и технологии в борбата с COVID-19 следва да се използват за овластяване на хората, а не за тяхното контролиране, стигматизиране или репресиране. Освен това, макар че данните и технологиите могат да представляват важни инструменти, те имат и някои присъщи ограничения и могат просто да повишат ефективността на други мерки в областта на общественото здраве. Общите принципи на ефективност, необходимост и пропорционалност трябва да обуславят всяка мярка, която държавите членки или институциите на ЕС приемат и която включва обработване на лични данни за борба с COVID-19.

5 В настоящите насоки се пояснява условията и принципите за пропорционалното използване на данните за местонахождение и на инструментите за проследяване на контакти за две конкретни цели:

- използване на данните за местонахождение в подкрепа на борбата с пандемията чрез моделиране на разпространението на вируса, така че да се оцени общата ефективност на мерките за изолация;

1 Позоваванията на „държавите членки“ в настоящия документ следва да се разбират като позовавания на „държавите — членки на ЕИП“.

- проследяване на контактите, като целта е физическите лица да бъдат уведомявани, че са били в непосредствена близост до някого, за когото в крайна сметка е потвърдено, че е носител на вируса, така че веригите на заразяване да се прекъснат на възможно най-ранен етап.

6 Ефективният принос на приложенията за проследяване на контакти за справянето с пандемията зависи от множество фактори (например процента на хората, които трябва да инсталират съответното приложение; определението на „контакт“ от гледна точка на близостта и продължителността). Освен това такива приложенията трябва да са част от всеобхватна стратегия за обществено здравеопазване, предназначена за борба с пандемията, която да включва, наред с другото, изследването и последващото неавтоматизирано проследяване на контакти, за да отпаднат съмненията. Внедряването на такива приложения следва да се съпътства от подкрепящи мерки, за да се гарантира, че предоставената на ползвателите информация е контекстуализирана и че предупрежденията могат да бъдат полезни за системата на общественото здравеопазване. В противен случай може да не се постигне пълното въздействие от използването на тези приложения.

7 ЕКЗД подчертава, че както в ОРЗД, така и в Директива 2002/58/ЕО (наричана по-нататък „Директивата“) се съдържат специални правила, които позволяват използването на анонимни или лични данни за подпомагане на публичните органи и други субекти на национално равнище и на равнище ЕС в наблюдението и овладяването на разпространението на вируса SARS-CoV-2[2].

8 В това отношение ЕКЗД вече изрази позицията си по отношение на факта, че използването на приложения за проследяване на контакти следва да бъде доброволно и че тези приложения не бива да проследяват конкретните движения на физическите лица, а да разчитат по-скоро на информация за хора и обекти в непосредствена близост до ползвателите[3].

[2] Вж. предишното изявление на ЕКЗД относно пандемията от COVID-19.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 ИЗПОЛЗВАНЕ НА ДАННИ ЗА МЕСТОНАХОЖДЕНИЕ

2.1 Източници на данни за местонахождение

9 Съществуват два основни източника на данни за местонахождение, които могат да се използват за моделиране на разпространението на вируса и за повишаване на общата ефективност на мерките за изолация:

- данните за местонахождение, събирани от доставчиците на електронни съобщителни услуги (например операторите на мобилни далекосъобщителни услуги) в контекста на предоставянето на техните услуги; и
- данните за местонахождение, събирани от приложенията на доставчиците на услуги на информационното общество, чието функциониране изисква използването на такива данни (например навигация, услуги за превоз и др.).

10 ЕКЗД припомня, че данните за местонахождение[4], събирани чрез доставчиците на електронни съобщителни услуги, могат да се обработват само в съответствие с членове 6 и 9 от Директивата. Това означава, че тези данни могат да се предават на органите или на други трети страни само ако са анонимизирани от доставчика или — когато става въпрос за данни, указващи географското положение на крайното оборудване на ползвателя, които не представляват данни за трафик — само с предварителното съгласие на ползвателите[5].

11 По отношение на информацията, включително данните за местонахождение, събирани директно от крайното оборудване, се прилага член 5, параграф 3 от Директивата. По този начин съхраняването на информация в устройството на ползвателя или получаването на достъп до информация, вече съхранявана в неговото устройство, се позволява само ако i) ползвателят е дал своето съгласие[6] или ii) съхранението и/или достъпът са строго необходими за предоставяне на изрично поисканата от ползвателя услуга на информационното общество.

12 В съответствие с член 15 обаче са възможни дерогации от правата и задълженията, предвидени в Директивата, когато те представляват необходима, подходяща и пропорционална мярка в рамките на демократично общество за определени цели[7].

13 Що се отнася до повторното използване на данните за местонахождение, събирани от доставчик на услуга на информационното общество, за свързани с моделиране цели (например чрез операционната система или друго, инсталирано преди това приложение), трябва да бъдат изпълнени допълнителни условия. В действителност, когато данните са събрани в съответствие с член 5, параграф 3 от Директивата, по-нататъшното им обработване е възможно само с допълнителното съгласие на субекта на данни или въз основа на законодателен акт на Съюза или на държава членка, който представлява необходима и пропорционална мярка в рамките на демократично общество, за да се гарантират целите, посочени в член 23, параграф 1 от ОРЗД[8].

2.2 Акцент върху използването на анонимизирани данни за местонахождение

14 ЕКЗД подчертава, че при използването на данни за местонахождение следва винаги да се отдава предпочитание на обработването на анонимизирани, а не на лични данни.

---

[4] Вж. член 2, буква в) от Директивата.
[5] Вж. членове 6 и 9 от Директивата.
[6] Понятието за съгласие в Директивата е същото като понятието за съгласие в ОРЗД и трябва да отговаря на всички изисквания по отношение на съгласието, предвидени в член 4, параграф 11 и член 7 от ОРЗД.
[7] За тълкуването на член 15 от Директивата вж. също решение на Съда на ЕС от 29 януари 2008 г. по дело C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU.
[8] Вж. раздел 1.5.3 от Насоки № 1/2020 относно обработването на лични данни в контекста на свързаните превозни средства.

15 Анонимизация означава използването на набор от техники, чрез които се елиминира възможността чрез „разумно вероятни“ усилия да се направи връзка между данните и физическо лице, което е идентифицирано или може да бъде идентифицирано. При тази „проверка за разумна вероятност“ трябва да се отчитат както обективните аспекти (време, технически средства), така и контекстуалните елементи, които могат да бъдат различни за всеки отделен случай (рядкост на дадено явление, като се отчита например гъстотата на населението, естеството и обемът на данните). Ако данните не преминат успешно през тази проверка, това ще означава, че те не са анонимизирани и следователно продължават да бъдат в обхвата на ОРЗД.

16 Оценката дали анонимизацията е надеждна зависи от три критерия: i) възможността за посочване (изолиране на физическо лице в рамките на по-голяма група въз основа на данните); ii) възможността за свързване (свързване на два записа, отнасящи се до едно и също лице); и iii) достигането до изводи (извеждане по дедуктивен път на неизвестна информация със значителна степен на вероятност относно физическо лице).

17 В много случаи понятието за анонимизация не се разбира правилно и често се бърка с псевдонимизация. Докато анонимизацията позволява данните да се използват без никакви ограничения, псевдонимизираните данни продължават да бъдат в обхвата на ОРЗД.

18 Съществуват много варианти за ефективна анонимизация[9], но при едно условие. Данните не е възможно да се анонимизират самостоятелно, което означава, че само цели набори от данни могат да се анонимизират или не. В този смисъл всяка намеса по отношение на отделен елемент от данни (чрез криптиране или други математически преобразувания) може в най-добрия случай да се счита за псевдонимизация.

19 Процесите на анонимизация и атаките за повторно установяване на самоличността представляват области, в които активно се извършват изследвания. От огромно значение за всеки администратор на данни, който прилага решения за анонимизация, е да следи най-новите развития в тази област, особено във връзка с данните за местонахождение (с произход от оператори на далекосъобщителни услуги и/или услуги на информационното общество), за които е известно, че са особено трудни за анонимизиране.

20 В действителност множество изследвания показват[10], че *данните за местонахождение, които се считат за анонимизирани,* всъщност може и да не са. За следите от мобилността на физическите лица е присъщо, че са уникални и с висока степен на корелация. Поради това при определени обстоятелства те могат да бъдат уязвими при опити за повторно установяване на самоличността.

21 Отделен елемент на данни, който проследява местонахождението на физическо лице в рамките на значителен период от време, не може да бъде анонимизиран напълно. Този извод може да остане валиден, ако прецизността на записваните географски координати не бъде понижена в достатъчна степен или ако се премахнат подробностите във връзка с маршрута и дори ако се запази само информацията за местата, където субектът на данни прекарва значителни периоди от време. Това важи и за данните за местонахождение, които не са агрегирани в достатъчна степен.

22 За да се постигне анонимизация, данните за местонахождение трябва да бъдат внимателно обработени, за да преминат успешно проверката за разумна вероятност. В този смисъл такова обработване включва отчитането на наборите с данни за местонахождение като цяло, както и обработване на данни от разумно голям набор от

---

[9] (de Montjoye et al., 2018 г.) „On the privacy-conscientious use of mobile phone data“.
[10] (de Montjoye et al., 2013 г.) Unique in the Crowd: The privacy bounds of human mobility и (Pyrgelis et al., 2017 г.) Knock Knock, Who’s There? Membership Inference on Aggregate Location Data

лица, като се използват наличните надеждни техники за анонимизация, при условие че те се прилагат по правилен и ефективен начин.

23 На последно място, с оглед на сложността на процесите за анонимизация е силно препоръчително да се осигури прозрачност по отношение на методологията за анонимизация.

3 ПРИЛОЖЕНИЯ ЗА ПРОСЛЕДЯВАНЕ НА КОНТАКТИ

3.1 Общ правен анализ

24 Системното и мащабно наблюдение на местонахождението и/или контактите между физически лица представлява сериозно нарушение на неприкосновеността на личния им живот. То може да бъде легитимно само ако се основава на доброволното му приемане от потребителите за всяка от определените цели. По-специално това предполага, че лицата, които решат да не използват такива приложения или които не могат да ги използват, не следва по никакъв начин да бъдат поставени в неблагоприятно положение.

25 За да се гарантира отчетността, следва ясно да се определи администраторът на данни за всяко приложение за проследяване на контакти. ЕКЗД счита, че националните здравни органи биха могли да изпълняват ролята на администратори на данни[11] за такива приложения, като могат да се предвидят и други администратори. Във всеки случай, ако внедряването на приложения за проследяване на контакти включва различни субекти, техните роли и отговорности трябва да бъдат ясно определени от самото начало и да бъдат обяснени на потребителите.

26 В допълнение към това, предвид принципа на ограничаване в рамките на целта, целите трябва да бъдат достатъчно конкретни, така че да се изключи възможността за допълнително обработване на данните за цели, които не са свързани с управлението на здравната криза, предизвикана от COVID-19 (например за търговски цели или за цели на правоприлагането). След като целта бъде ясно определена, ще трябва да се гарантира, че използването на лични данни е подходящо, необходимо и пропорционално.

27 В контекста на приложение за проследяване на контакти следва да се отчетат внимателно принципът на свеждане на данните до минимум, както и защитата на данните на етапа на проектирането и по подразбиране:

- приложенията за проследяване на контакти не изискват проследяването на местонахождението на отделните ползватели. Вместо това следва да се използват данни за хора и обекти в непосредствена близост до ползвателите;
- тъй като приложенията за проследяване на контакти могат да функционират без прякото установяване на самоличността на отделни лица, следва да се въведат подходящи мерки за предотвратяване на повторното установяване на самоличността;
- събраната информация следва да се съхранява в крайното оборудване на ползвателя и следва да се събира само уместната информация, когато това е абсолютно необходимо.

28 Що се отнася до законосъобразността на обработването на данни, ЕКЗД отбелязва, че приложенията за проследяване на контакти предполагат съхранението и/или достъпа до информация, която вече се съхранява в крайното оборудване и която е уредена с член 5, параграф 3 от Директивата. Ако тези операции са абсолютно необходими, за да може доставчикът на приложението да предостави изрично поисканата от ползвателя услуга, за обработването няма да се изисква съгласието на последния. За операции, които не са абсолютно необходими, доставчикът ще трябва да получи съгласието на ползвателя.

29 Освен това ЕКЗД отбелязва, че сам по себе си фактът, че използването на приложения за проследяване на контакти е доброволно, не означава, че обработването на лични данни непременно ще се основава на съгласие. Когато публичните органи предоставят услуга, основана на мандат, възложен им по закон и отговарящ на законоопределени изисквания, изглежда, че най-уместното правно основание за обработването на данни е

[11] Вж. също Европейска комисия, „Насоки за мобилните приложения, които подпомагат борбата с пандемията от COVID-19, във връзка със защитата на данните“, Брюксел, 16.4.2020 г., C(2020) 2523 final.

то да е необходимо за изпълнението на задача от обществен интерес, т.е. член 6, параграф 1, буква д) от ОРЗД.

30 В член 6, параграф 3 от ОРЗД се пояснява, че основанието за обработването на данни, посочено в член 6, параграф 1, буква д), трябва да е установено от правото на Съюза или правото на държавата членка, което се прилага спрямо администратора. Целта на обработването се определя в това правно основание или, доколкото се отнася до обработването по параграф 1, буква д), то трябва да е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора[12].

31 Правното основание или законодателната мярка, които представляват законното основание за използването на приложения за проследяване на контакти, обаче следва да включват смислени предпазни мерки, включително позоваване на доброволното естество на приложението. Следва да се посочат ясно целта и изричните ограничения във връзка с допълнителното използване на лични данни, както и ясно да се обозначи съответният администратор или администратори. Освен това следва да се идентифицират категориите данни и субектите, на които могат да се разкриват личните данни (както и целите, за които може да се прави това). В зависимост от степента на вмешателство, следва да се внедрят допълнителни предпазни мерки, като се отчитат естеството, обхватът и целите на обработването. На последно място ЕКЗД също така препоръчва, веднага щом това е осъществимо, да се включат критерии, с които да се определи кога ще бъде преустановено използването на приложението и кой субект ще е отговорен и подотчетен за това решение.

32 Ако обаче обработването на данни се извършва съгласно друго правно основание, като например даването на съгласие (член 6, параграф 1, буква а)[13], администраторът ще трябва да гарантира, че са изпълнени строгите изисквания за валидността на това правно основание.

33 Освен това използването на приложение за борба с пандемията с COVID-19 може да доведе до събирането на данни за здравословното състояние (например дали дадено лице е заразено). Обработването на такива данни е разрешено, когато то е необходимо от съображения от обществен интерес в областта на общественото здраве, като отговаря на условията на член 9, параграф 2, буква и) от ОРЗД[14], или е необходимо за цели, свързани с осигуряването на здравни грижи, както са описани в член 9, параграф 2, буква з) от ОРЗД[15]. В зависимост от правното основание, обработването може да бъде основано и на даването на изрично съгласие (член 9, параграф 2, буква а) от ОРЗД).

34 В съответствие с първоначалната цел член 9, параграф 2, буква й) от ОРЗД също така позволява да се обработват данни за здравословното състояние, когато това е необходимо за научни изследвания или за статистически цели.

35 Настоящата здравна криза не следва да се използва като възможност за установяване на непропорционални правомощия за запазване на данни. При ограничаването на съхранението следва да се отчетат реалните нужди и медицинската значимост (това може да включва мотивирани от епидемиологична гледна точка съображения като инкубационния период и др.), като личните данни следва да се съхраняват само докато трае кризата с COVID-19. Като общо правило след това всички лични данни следва да бъдат изтрити или анонимизирани.

---

[12] Вж. съображение 41.

[13] Администраторите (и особено публичните органи) трябва да обърнат специално внимание на факта, че съгласието не следва да се разглежда като свободно дадено, ако лицето няма истински избор да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него.

[14] Обработването на данни трябва да бъде основано на правото на Съюза или правото на държава членка, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните, по-специално опазването на професионална тайна.

[15] Вж. член 9, параграф 2, буква з) от ОРЗД.

36 Според ЕКЗД такива приложения не могат да заменят, а само да подпомогнат неавтоматизираното проследяване на контакти, което се извършва от квалифициран персонал в сферата на общественото здравеопазване, който може да прецени дали има вероятност близките контакти да доведат до предаване на вируса или не (например при общуване с лица, защитени с подходящи средства, като касиери и др., или с лица, които не са защитени). ЕКЗД подчертава, че процедурите и процесите, включващи съответните алгоритми, които се използват от приложенията за проследяване на контакти, следва да се прилагат под строгия надзор на квалифициран персонал, за да се ограничи възникването на фалшиви положителни и отрицателни резултати. По-специално задачата за предоставяне на съвети относно следващите стъпки не следва да се основава единствено на автоматизирано обработване на данни.

37 За да се гарантира, че алгоритмите са справедливи, подлежат на отчетност и са в съответствие със закона в по-широк план, те трябва да позволяват извършването на одити и следва да се подлагат на редовни прегледи от независими експерти. Изходният код на приложението следва да е публично достъпен, за да се осигури възможно най-широк надзор.

38 Получаването на известен брой фалшиви положителни резултати е неизбежно. Тъй като идентифицирането на риск от заразяване има вероятност да окаже сериозно въздействие върху физическите лица, като например самоизолиране до получаване на отрицателен резултат от изследване, трябва да съществува възможност за коригиране на данните и/или на резултати от последващи анализи. Разбира се, това следва да важи само в ситуации и варианти на прилагане, при които данните се обработват и/или съхраняват по такъв начин, че коригирането е технически осъществимо, и има вероятност от настъпване на неблагоприятните ефекти, посочени по-горе.

39 На последно място ЕКЗД счита, че преди внедряването на такива инструменти трябва да се извърши оценка на въздействието върху защитата на данните (ОВЗД), защото се счита, че съществува вероятност обработването да породи висок риск (данни за здравословното състояние, очаквано мащабно внедряване, системно наблюдение, използване на ново технологично решение)[16]. ЕКЗД настоятелно препоръчва ОВЗД да се публикуват.

3.2 Препоръки и функционални изисквания

40 В съответствие с принципа за свеждане на данните до минимум, измежду другите мерки за защита на данните на етапа на проектирането и по подразбиране[17], обработваните данни следва да бъдат сведени до абсолютния минимум. Приложението не следва да събира несвързана или ненужна информация, която може да включва гражданско състояние, комуникационни идентификатори, информация от телефонния указател на устройството, съобщения, записи за повиквания, данни за местонахождение, идентификатори на устройства и др.

41 Излъчваните от приложенията данни трябва да включват единствено някои уникални и псевдонимни идентификатори, които се генерират от приложението и са специфични за него. Тези идентификатори трябва периодично да се обновяват, с честота, която е съвместима с целта да се ограничи разпространението на вируса и е достатъчна за ограничаване на риска от идентифициране и физическо проследяване на отделни лица.

---

[16] Вж. Насоки на Работната група за защита на личните данни по член 29 (приети от ЕКЗД) относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679.

[17] Вж. Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране съгласно член 25.

42 При вариантите за проследяване на контакти може да се следва централизиран или децентрализиран подход[18]. И двата подхода следва да се считат за осъществими варианти, при условие че са въведени подходящи мерки за сигурност, като всеки от тях се характеризира с определени предимства и недостатъци. Поради това концептуалният етап от разработването на приложение следва винаги да включва задълбочено проучване и на двете концепции, като се съпоставят внимателно съответните им ефекти върху защитата на данните/неприкосновеността на личния живот и възможните въздействия върху правата на физическите лица.

43 На всеки сървър, включен в системата за проследяване на контакти, трябва да се съхранява само хронологията на контактите или псевдонимните идентификатори на ползвател, диагностициран като заразен вследствие на подходяща оценка от здравните органи и на доброволно действие от страна на ползвателя. Като алтернативен вариант, на сървъра трябва да се съхранява списък с псевдонимни идентификатори на заразени ползватели и хронологията на контактите им само за периода от време, който е необходим за информиране на потенциално заразените ползватели за факта, че са били изложени на вируса, и не следва да се правят опити да се идентифицират потенциално заразени ползватели.

44 Въвеждането на глобална методология за проследяване на контакти, която включва както мобилни приложения, така и неавтоматизирано проследяване, в някои случаи може да налага обработването на допълнителна информация. В този контекст допълнителната информация следва да се съхранява в устройството на ползвателя и да се обработва само когато това е абсолютно необходимо и с неговото предварително и изрично съгласие.

45 За да се гарантира сигурността на данните, съхранявани в сървърите и приложенията, както и на обмена на данни между приложенията и отдалечения сървър, трябва да се използват най-съвременните криптографски техники. Освен това трябва да се извършва взаимна автентификация между приложението и сървъра.

46 Докладването на ползватели в приложението като заразени със SARS-CoV-2 трябва да подлежи на надлежно разрешение, например чрез код за еднократна употреба, обвързан с псевдонимната самоличност на заразеното лице и свързан с лаборатория за изследване или със здравен специалист. Ако не е възможно да се получи потвърждение по сигурен начин, не следва да се извършва обработване на данни, при което се приема, че ползвателят със сигурност е или не е заразен.

47 В сътрудничество с публичните органи администраторът трябва ясно и изрично да посочи връзката в интернет, от която да се изтегли официалното национално приложение за проследяване на контакти, за да се смекчи рискът от използване на приложение на трета страна.

[18] По принцип децентрализираното решение съответства в по-голяма степен на принципа на свеждане на данните до минимум.

4 ЗАКЛЮЧЕНИЕ

48 Светът е изправен пред безпрецедентна криза в сферата на общественото здравеопазване, налагаща решителни мерки, които ще продължат да оказват въздействие и след настоящата извънредна ситуация. Автоматизираното обработване на данни и цифровите технологии могат да бъдат ключови елементи в борбата с COVID-19. Следва обаче да се внимава за т. нар. „ефект на храповия механизъм“ (инерционен ефект). Наша отговорност е да гарантираме, че всички мерки, предприети при тези извънредни обстоятелства, са необходими, ограничени във времето, с минимален обхват и подлежащи на периодичен и безпристрастен преглед, както и на научна оценка.

49 ЕКЗД подчертава, че не следва да се налага да се прави избор между ефективността на отговора на настоящата криза и защитата на основните ни права: можем да постигнем и двете, като освен това принципите за защита на данните могат да имат изключително важна роля в борбата с вируса. Европейското законодателство за защита на данните позволява отговорното използване на лични данни с цел управление на здравето, като същевременно гарантира, че в рамките на този процес не се подронват индивидуалните права и свободи.

За Европейския комитет по защита на данните,

Председател

(Andrea Jelinek)

ПРИЛОЖЕНИЕ — МОБИЛНИ ПРИЛОЖЕНИЯ ЗА ПРОСЛЕДЯВАНЕ НА КОНТАКТИ
РЪКОВОДСТВО ЗА АНАЛИЗ

0. Отказ от отговорност

Следните насоки не са нито задължителни, нито изчерпателни, като единствената цел на настоящото ръководство е да се предоставят общи насоки за лицата, които проектират и внедряват мобилни приложения за проследяване на контакти. Могат да се използват и други решения, различни от описаните тук, като те също могат да са законосъобразни, ако спазват съответната правна уредба (т.е. ОРЗД и Директивата).

Трябва също да се отбележи, че настоящото ръководство е с общ характер. В съответствие с това съдържащите се в него препоръки и задължения не трябва да се считат за изчерпателни. За всеки конкретен случай трябва да се извършва отделна оценка, като някои конкретни приложения може да изискват допълнителни мерки, които не са включени в настоящото ръководство.

1. Резюме

В много държави членки заинтересованите страни обмислят използването на мобилни приложения за *проследяване на контакти*, за да се помогне на гражданите да установят дали са били в контакт с лице, заразено със SARS-CoV-2.

Все още не са установени условията, при които такива приложения биха допринесли ефективно за справяне с пандемията. Тези условия ще трябва да се установят преди въвеждането на такова приложение. Въпреки това е уместно да се предоставят насоки, чрез които да се осигури подходяща информация на разработващите екипи нагоре по веригата, така че защитата на личните данни да може да се гарантира от ранния етап на проектирането.

Трябва да се отбележи, че настоящото ръководство е с общ характер. В съответствие с това съдържащите се в него препоръки и задължения не трябва да се считат за изчерпателни. За всеки конкретен случай трябва да се извършва отделна оценка, като някои конкретни приложения може да изискват допълнителни мерки, които не са включени в настоящото ръководство. Целта на настоящото ръководство е да се предоставят общи насоки за лицата, които проектират и внедряват мобилни приложения за проследяване на контакти.

Възможно е някои критерии да надхвърлят строгите изисквания, произтичащи от уредбата за защита на личните данни. Тяхната цел е да се гарантира възможно най-високо ниво на прозрачност, което ще благоприятства общественото одобрение на такива приложения за проследяване на контакти.

За тази цел създателите на приложения за проследяване на контакти следва да вземат предвид следните критерии:

- Използването на такова приложение трябва да е абсолютно доброволно. То не може да обуславя достъпа до каквито и да е права, гарантирани от закона. Физическите лица трябва да разполагат с пълен контрол върху своите данни във всеки момент и следва да са в състояние да избират свободно дали да използват такова приложение.

- Има вероятност приложенията за проследяване на контакти да породят голям риск за правата и свободите на физическите лица и да се наложи извършването на оценка на въздействието върху защитата на данните, преди да бъдат внедрени.

- Информацията дали ползвателите на приложението се намират в непосредствена близост може да бъде получена и без установяване на тяхното местонахождение. Следователно този вид приложение не изисква и поради това не следва да включва използването на данни за местонахождение.

- Когато даден ползвател бъде диагностициран като заразен със SARS-CoV-2, следва да бъдат информирани само лицата, с които е бил в тесен контакт през епидемиологично значимия период, за който се запазват данни с цел проследяване на контактите.

- В зависимост от избраната архитектура, за функционирането на такъв вид приложение може да е необходим централизиран сървър. В такъв случай и в съответствие с принципа на свеждане на данните до минимум и принципа на защитата на данните на етапа на проектирането, обработваните от централизирания сървър данни следва да бъдат ограничени до абсолютния минимум:

    - Когато даден ползвател бъде диагностициран като заразен, информацията относно предишните му тесни контакти или идентификаторите, излъчвани от използваното от него приложение, могат да се събират само с негово съгласие. Трябва да бъде установен метод за проверка, който позволява да се потвърди, че съответното лице действително е заразено, без да се установява неговата самоличност като ползвател. Технически това би могло да се постигне чрез известяване на контактите само след намесата на здравен специалист, например чрез използване на специален еднократен код.

    - Информацията, която се съхранява на централния сървър, не следва да позволява на администратора нито да идентифицира диагностицираните като заразени ползватели или лицата, които са били в контакт с такива ползватели, нито да извежда елементи от данни за контакти, които не са необходими за определяне на значимите в случая контакти.

- За функционирането на такъв вид приложение е необходимо излъчването на данни, които да се четат от устройствата на други ползватели, както и прослушването на тези излъчени данни:

    - е достатъчно да се обменят псевдонимни идентификатори между мобилните устройства на ползвателите (компютри, таблети, свързани часовници и др.), например чрез излъчването им (например чрез технологията Bluetooth Low Energy);

    - идентификаторите трябва да се генерират с използване на най-съвременни криптографски процеси;

    - идентификаторите трябва периодично да се обновяват, за да се намали рискът от физическо проследяване и атаки за повторно установяване на самоличността.

- Този вид приложение трябва да бъде защитено, за да се гарантира безопасното осъществяване на техническите процеси. По-специално:

- Приложението не следва да предава на ползвателите информация, която им позволява да отгатват самоличността или диагнозата на други лица. Централният сървър не трябва нито да идентифицира ползвателите, нито да извежда информация за тях по дедуктивен път.

Отказ от отговорност: горепосочените принципи са свързани с декларираната цел на приложенията за *проследяване на контакти* и само с тази цел, единственото предназначение на която е автоматичното информиране на потенциално изложени на вируса лица (без да е необходимо да се установява тяхната самоличност).Компетентният надзорен орган може да контролира операторите на приложението и неговата инфраструктура. Следването на всички посочени насоки или на част от тях не е непременно достатъчно, за да се гарантира пълното съответствие с уредбата за защита на данните.

2. Определения

Контакт	В контекста на мобилно приложение за проследяване на контакти контактът е ползвател, общувал с друг ползвател, за когото е потвърдено, че е носител на вируса, като продължителността и разстоянието при това общуване пораждат риск от значително излагане на вирусната инфекция. Параметрите за продължителността на излагането и разстоянието между хората трябва да бъдат определени от здравните органи и могат да бъдат зададени в приложението.
Данни за местонахождение	Става въпрос за всички данни, които се обработват в електронна съобщителна мрежа или чрез електронна съобщителна услуга и които указват географското местоположение на крайното оборудване на ползвателя на обществено достъпна електронна съобщителна услуга (съгласно определението в Директивата), както и данни от потенциални други източници, свързани със: • географската ширина, географската дължина или надморската височина, на която се намира крайното оборудване; • посоката, в която се придвижва ползвателят; или • момента, в който е записана информацията за местонахождението.
Взаимодействие	В контекста на приложението за проследяване на контакти взаимодействието се определя като обмена на информация между две устройства, разположени в непосредствена близост едно до друго (във времето и пространството), в рамките на обхвата на използваната комуникационна технология (например Bluetooth). Това определение изключва местонахождението на двамата ползватели, осъществяващи взаимодействието.
Носител на вируса	В настоящия документ определяме носителите на вируса като ползватели, които са дали положителна проба за вируса и които са получили официална диагноза от лекар или здравен център.

Проследяване на контакти	Хората, които са били в тесен контакт (в съответствие с критерии, които трябва да бъдат определени от епидемиолози) с лице, заразено с вируса, могат да бъдат изложени на значителен риск от заразяване и на свой ред да заразят други лица. Проследяването на контактите представлява методология за контрол на заболявания, при която се прави списък на всички лица, които са били в непосредствена близост до носител на вируса, за да се провери дали са изложени на риск от заразяване и да се предприемат подходящи санитарни мерки спрямо тях.

3. Общи положения

GEN-1	Приложението трябва да е инструмент, който допълва традиционните техники за проследяване на контакти (а именно събеседвания а със заразени лица), т.е. да е част от по-широкообхватна програма в областта на общественото здравеопазване. То трябва да се използва само до момента, в който броят на новите случаи на заразени лица може да се отчита и само с неавтоматизирани техники за проследяване на контакти.
GEN-2	Най-късно към момента, в който компетентните публични органи вземат решение за връщане към нормалните условия на живот, трябва да се установи процедура, чрез която да се спре събирането на идентификатори (глобално деактивиране на приложението, указания за деинсталиране на приложението, автоматично деинсталиране и др.) и да се пристъпи към изтриването на всички събрани данни от всички бази данни (мобилни приложения и сървъри).
GEN-3	Изходният код на приложението и неговият бекенд трябва да бъдат отворени и техническите спецификации трябва да бъдат публични, така че всяка заинтересована страна да може да провери кода и по целесъобразност да допринесе за подобряването му, за коригирането на евентуални грешки и за осигуряването на прозрачност при обработването на лични данни.
GEN-4	Етапите на внедряване на приложението трябва да позволяват постепенното валидиране на неговата ефективност от гледна точка на общественото здраве. За тази цел нагоре по веригата трябва да се определи протокол за оценка, в който се посочват показатели, позволяващи да се прецени ефективността на приложението.

4. Цели

PUR-1	Единствената цел на приложението трябва да бъде проследяването на контактите, така че да могат хората, потенциално изложени на SARS-CoV-2,

	да бъдат известени и да им се окажат необходимите грижи. То не трябва да се използва за друга цел.
PUR-2	Приложението не трябва да бъде отклонявано от първоначалната му цел към наблюдение на спазването на карантинните или изолационните мерки и/или социалното дистанциране.
PUR-3	То не трябва да се използва за достигане до заключения относно местонахождението на ползвателите въз основа на техните взаимодействия и/или чрез каквито и да е други средства.

5. Функционални съображения

FUNC-1	Приложението трябва да осигурява функция, която да позволява ползвателите да бъдат информирани, че са били потенциално изложени на вируса, като тази информация се основава на непосредствената близост до заразен ползвател в рамките на срок от X дни преди положителното скринингово изследване (стойността X се определя от здравните органи).
FUNC-2	Приложението следва да дава препоръки на ползвателите, за които е установено, че са били потенциално изложени на вируса. То следва да дава указания във връзка с мерките, които ползвателите следва да предприемат и да позволява на ползвателя да потърси съвети. В такива случаи човешката намеса ще бъде задължителна.
FUNC-3	Алгоритъмът, който измерва риска от заразяване, като отчита факторите разстояние и време и по този начин определя кога даден контакт трябва да се отбележи в списъка за проследяване на контакти, трябва да може да се настройва по сигурен начин, така че да се отчитат най-новите знания относно разпространението на вируса.
FUNC-4	**Ползвателите трябва да бъдат информирани, в случай че са били изложени на вируса**, или трябва редовно да получават информация дали са били изложени на вируса или не в рамките на инкубационния му период.
FUNC-5	Приложението следва да бъде оперативно съвместимо с други приложения, разработени в рамките на държавите членки, така че да е възможно ползвателите, които пътуват от една държава членка до друга, да бъдат уведомявани по ефикасен начин.

6. Данни

DATA-1	Приложението трябва да е в състояние да излъчва и получава данни чрез комуникационни технологии за работа в непосредствена близост като Bluetooth Low Energy с цел да се извършва проследяването на контактите.

DATA-2	Излъчваните данни трябва да включват псевдослучайни идентификатори с висока степен на криптографска сигурност, които се генерират от приложението и са специфични за него.
DATA-3	Рискът от стълкновение между псевдослучайните идентификатори следва да е достатъчно нисък.
DATA-4	Псевдослучайните идентификатори трябва периодично да се обновяват, с честота, която е достатъчна за ограничаване на риска от повторно установяване на самоличността, физическо проследяване или свързване на отделни хора от което и да е лице, включително от операторите на централния сървър, от други ползватели на приложението или от злонамерени трети страни. Тези идентификатори трябва да се генерират от приложението на ползвателя, евентуално въз основа на сийд (seed), осигурен от централния сървър.
DATA-5	В съответствие с принципа на свеждане на данните до минимум приложението не трябва да събира други данни, освен абсолютно необходимите за проследяването на контактите.
DATA-6	Приложението не трябва да събира данни за местонахождение с цел проследяване на контактите. Данни за местонахождение могат да се обработват единствено с цел да се позволи на приложението да взаимодейства с подобни приложения в други държави и тяхната точност следва да бъде ограничена до абсолютно необходимото за тази единствена цел.
DATA-7	Приложението не следва да събира данни за здравословното състояние в допълнение към данните, които са абсолютно необходими за целите на приложението, освен на доброволна основа, като единствената цел следва да бъде подпомагането на процеса на вземане на решение за информиране на ползвателя.
DATA-8	Ползвателите трябва да бъдат информирани за всички лични данни, които ще бъдат събирани. Тези данни следва да се събират само с разрешението на ползвателя.

7. Технически характеристики

TECH-1	Приложението следва да използва налични технологии, като например комуникационни технологии за работа в непосредствена близост (например Bluetooth Low Energy), за да открива ползватели в околността на устройството, които също използват приложението.
TECH-2	То следва да съхранява хронологията на контактите на даден ползвател в оборудването за предварително определен и ограничен период от време.
TECH-3	Приложението може да разчита на централен сървър за изпълнението на някои функции.

TECH-4	То трябва да се основава на архитектура, при която се разчита във възможно най-голяма степен на устройствата на ползвателите.
TECH-5	По инициатива на ползватели, които са обявени за заразени с вируса, и след потвърждение на тяхното състояние от надлежно сертифициран здравен специалист, хронологията на техните контакти или техните собствени идентификатори следва да бъдат предадени на централния сървър.

8. Сигурност

SEC-1	Трябва да се въведе механизъм за проверка на състоянието на ползвателите, които обявяват в приложението, че са заразени със SARS-CoV-2, например чрез осигуряване на код за еднократна употреба, свързан с лаборатория за изследване или със здравен специалист. Ако не е възможно да се получи потвърждение по сигурен начин, данните следва да не се обработват.
SEC-2	Данните, които се изпращат до централния сървър, трябва да се предават по защитен канал. Следва да се подложи на внимателна оценка използването на услугите за уведомяване, предоставяни от доставчиците на ОС платформи, като те не следва да водят до разкриване на каквито и да е данни на трети страни.
SEC-3	Запитванията трябва да бъдат защитени спрямо манипулирането им от злонамерен ползвател.
SEC-4	Трябва да се използват най-съвременни криптографски техники, за да се обезопаси обменът на данни между приложението и сървъра и между отделните приложения, както и принципно да се защити информацията, съхранявана в приложенията и на сървъра. Примерите за техники, които могат да се използват, включват: симетрично и асиметрично криптиране, хеш функции, проверка дали даден елемент се съдържа в скрит набор от данни (Private Membership Test), сравнение на скрити набори от данни (Private Set Intersection), блум филтри (Bloom filters), извличане на информация без разкриване на конкретния елемент (Private Information Retrieval), хомоморфно криптиране и др.
SEC-5	Централният сървър не трябва да съхранява идентификаторите за мрежова връзка (например IP адреси) на ползвателите, включително на диагностицираните с вируса и на онези, които са предоставили хронологията на своите контакти или собствените си идентификатори.
SEC-6	За да се избегне представянето за друго лице или създаването на фалшиви ползватели, сървърът трябва да автентифицира приложението.
SEC-7	Приложението трябва автентифицира централния сървър.
SEC-8	Функциите на сървъра трябва да са защитени от атаки с повторно възпроизвеждане (replay attacks).
SEC-9	Информацията, която се предава от централния сървър, трябва да е придружена от подпис, за да се автентифицират нейният произход и цялост.
SEC-10	Достъпът до всички данни, които се съхраняват в централния сървър и не са публично достъпни, трябва да е ограничен само до упълномощени лица.

SEC-11	Програмата за управление на разрешенията в устройството на нивото на операционната система трябва да отправя искания за необходимите разрешения само когато това е необходимо за осъществяването на достъп до и използването на комуникационните модули, за съхранението на данните в крайното оборудване и за извършването на обмен на информация с централния сървър.

9. Защита на личните данни и неприкосновеност на личния живот на физическите лица

Напомняне: насоките по-долу се отнасят до приложение, чиято единствена цел е проследяването на контакти.

PRIV-1	При обмена на данни трябва да се зачита неприкосновеността на личния живот на ползвателите (и по-специално да се спазва принципът на свеждане на данните до минимум).
PRIV-2	При използването на приложението не трябва да е възможно директното установяване на самоличността на ползвателите.
PRIV-3	Приложението не трябва да позволява проследяването на движенията на ползвателите.
PRIV-4	При използването на приложението ползвателите не следва да могат да научават никаква информация за други ползватели (и по-специално дали са носители на вируса или не).
PRIV-5	Доверието в централния сървър трябва да е ограничено. При управлението на централния сървър трябва да се следват ясно определени правила за управление и да се приложат всички необходими мерки за гарантиране на неговата сигурност. Локализацията на централния сървър следва да позволява ефективен надзор от компетентния надзорен орган.
PRIV-6	Трябва да се извърши оценка на въздействието върху защитата на данните, която следва да се оповести публично.
PRIV-7	Приложението следва да разкрива на ползвателя единствено дали е бил изложен на вируса, както и броя пъти и датите на излагане, по възможност без да разкрива информация за други ползватели.
PRIV-8	Предоставената от приложението информация не трябва да позволява на ползвателите да установяват самоличността на ползватели, заразени с вируса, нито техните движения.
PRIV-9	Предоставената от приложението информация не трябва да позволява на здравните органи да установяват самоличността на потенциално изложените на вируса ползватели без тяхното съгласие.
PRIV-10	Отправяните от приложението запитвания към централния сървър не трябва да разкриват никаква информация за носителя на вируса.
PRIV-11	Отправяните от приложението запитвания към централния сървър не трябва да разкриват никаква ненужна информация за ползвателя, освен евентуално и само при необходимост неговия псевдонимен идентификатор и списъка му с контакти.
PRIV-12	Не трябва да са възможни атаки за повторно установяване на самоличността.
PRIV-13	Ползвателите трябва да са в състояние да упражняват своите права чрез приложението.
PRIV-14	Изтриването на приложението трябва да води до изтриването на всички събрани на местно равнище данни.

PRIV-15	Приложението следва да събира само данните, които се предават от самото приложение или от оперативно съвместими равностойни приложения. Не се събират данни, свързани с други приложения и/или комуникационни устройства, излъчващи сигнали за проследяване в непосредствена близост.
PRIV-16	Следва да се използват прокси сървъри, за да се избегне повторното установяване на самоличността от централния сървър. Целта на тези *неучастващи в злонамерено договаряне сървъри* (non-colluding servers) е смесването на идентификаторите на няколко ползватели (както на носители на вируса, така и изпратените от отправящите запитвания) преди споделянето им с централния сървър, така че централният сървър да не може да разпознае идентификаторите (като например IP адреси) на ползвателите.
PRIV-17	Приложението и сървърът трябва да се разработят и конфигурират внимателно, така че да не събират никакви ненужни данни (например в сървърните дневници не следва да се включват идентификатори и др.) и да се избегне използването на пакети за разработка на софтуер (SDK) на трети страни, които събират данни за други цели.

Повечето приложения за проследяване на контакти, които се обсъждат понастоящем, по същество следват два подхода, когато даден ползвател бъде обявен за заразен: те могат или да изпратят до сървъра получената чрез сканиране хронология на контактите в непосредствена близост, или да изпратят списъка със собствени идентификатори, които са били излъчени. Следните принципи са формулирани в съответствие с тези два подхода. Макар че в настоящия документ се обсъждат именно тези подходи, това не означава, че не са възможни или дори не са за предпочитане други подходи, например такива, които използват някаква форма на E2E криптиране или други технологии за обезпечаване на сигурността или неприкосновеността на личния живот.

9.1. Принципи, които се прилагат само **когато приложението изпраща до сървъра списък с контакти**:

CON-1	Централният сървър трябва да събира хронологията на контактите на ползвателите, обявени за заразени със SARS-CoV-2, след доброволно действие от тяхна страна.
CON-2	Централният сървър не трябва да поддържа или да разпространява списък с псевдонимните идентификатори на ползвателите, заразени с вируса.
CON-3	Хронологията на контактите, която се съхранява на централния сървър, трябва да бъде изтрита след уведомяването на ползвателите, че са били в непосредствена близост до заразено с вируса лице.
CON-4	Данните не трябва да напускат оборудването на ползвателя с изключение на случаите, в които заразен с вируса ползвател сподели хронологията на своите контакти с централния сървър или ползвател отправи запитване до сървъра, за да установи дали е бил потенциално изложен на вируса.
CON-5	Всички идентификатори, включени в местната хронология, трябва да бъдат изтрити X дни след тяхното събиране (стойността X се определя от здравните органи).

CON-6	Хронологиите на контактите, предоставени от отделни ползватели, не следва да се обработват допълнително, например да се съпоставят с цел изграждане на глобални карти за непосредствена близост.
CON-7	Данните в сървърните дневници трябва да са сведени до минимум и да отговарят на изискванията за защита на данните.

9.2. Принципи, които се прилагат само когато приложението изпраща до сървъра списък със свои собствени идентификатори:

ID-1	Централният сървър трябва да събира излъчваните от приложението идентификатори на ползватели, обявени за заразени със SARS-CoV-2, след доброволно действие от тяхна страна.
ID-2	Централният сървър не трябва да поддържа или да разпространява хронологията на контактите на ползвателите, заразени с вируса.
ID-3	Идентификаторите, съхранявани на централния сървър, трябва да бъдат изтрити след разпространението им до другите приложения.
ID-4	Данните не трябва да напускат оборудването на ползвателя с изключение на случаите, в които заразен с вируса ползвател сподели своите идентификатори с централния сървър или ползвател отправи запитване до сървъра, за да установи дали е бил потенциално изложен на вируса.
ID-5	Данните в сървърните дневници трябва да са сведени до минимум и да отговарят на изискванията за защита на данните.