Официален вестник на Европейския съюз

C 124 I

Издание на български език

Информация и известия

Година 63

17 април 2020 г.

Съдържание

II *Съобщения*

СЪОБЩЕНИЯ НА ИНСТИТУЦИИТЕ, ОРГАНИТЕ, СЛУЖБИТЕ И АГЕНЦИИТЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ

Европейска комисия

2020/C 124 I/01 Съобщение на Комисията — Насоки за мобилните приложения, които подпомагат борбата с пандемията от COVID-19, във връзка със защитата на данните 1

BG

II

(Съобщения)

СЪОБЩЕНИЯ НА ИНСТИТУЦИИТЕ, ОРГАНИТЕ, СЛУЖБИТЕ И АГЕНЦИИТЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ

ЕВРОПЕЙСКА КОМИСИЯ

СЪОБЩЕНИЕ НА КОМИСИЯТА

Насоки за мобилните приложения, които подпомагат борбата с пандемията от COVID-19, във връзка със защитата на данните

(2020/C 124 I/01)

1 КОНТЕКСТ

Пандемията на COVID-19 изправи пред безпрецедентно предизвикателство Съюза, неговите държави членки и техните системи на здравеопазване, начин на живот, икономическа стабилност и ценности. Цифровите технологии и данни имат важна роля в борбата с кризата с COVID-19. Мобилните приложения, обикновено инсталирани на смартфони, могат да подпомогнат органите за обществено здравеопазване на национално равнище и на равнище ЕС при мониторинга и ограничаването на пандемията от COVID-19 и са от особено значение на етапа на отмяна на противоепидемичните мерки. Чрез тях могат да се предоставят преки насоки на гражданите и да се подкрепят усилията за проследяване на контактите. В редица държави — както в ЕС, така и в останалите части на света — национални или регионални органи или разработчици обявиха въвеждането на мобилни приложения, разполагащи с различни функции, които имат за цел да се съдейства за борбата с вируса.

На 8 април 2020 г. Комисията прие Препоръка относно общ инструментариум на Съюза за използване на технологии и данни за борба с кризата, породена от COVID-19, и за нейното преодоляване, и по-специално относно мобилните приложения и използването на анонимизирани данни за мобилността (наричана по-нататък „Препоръката“) ([1]). Целта на Препоръката е, наред с другото, да се разработи общ европейски подход („инструментариум“) за използването на мобилни приложения, координиран на равнището на ЕС, с цел предоставяне на възможности на гражданите да предприемат ефективни мерки за социално дистанциране, както и с цел предупреждаване, превенция и проследяване на контактите, така че да се спомогне за ограничаване на разпространението на заболяването COVID-19. В Препоръката се определят общите принципи, които следва да ръководят разработването на такъв инструментариум, и се посочва, че Комисията ще публикува допълнителни насоки, включително относно защитата на личните данни и последиците за неприкосновеността на личния живот от използването на мобилни приложения в тази област.

Със съвместната европейска пътна карта за отмяна на противоепидемичните мерки във връзка с COVID-19 Комисията, в сътрудничество с председателя на Европейския съвет, определи набор от принципи за постепенната отмяна на противоепидемичните мерки, въведени вследствие на разпространението на COVID-19. Мобилните приложения, включително функциите им за проследяване на контактите, могат да играят важна роля в този контекст. В зависимост от функциите, с които разполагат, и от това доколко населението ги използва тези приложения могат да имат значителен ефект върху диагностицирането, лечението и контрола на COVID-19 във и извън болнична среда. Те са от особено значение при отмяна на противоепидемичните мерки и когато рискът от заразяване се увеличи, тъй като все повече хора имат контакт помежду си. Тези приложения могат да спомогнат за прекъсване на веригите на заразяване по-бързо и по-ефикасно, отколкото общите противоепидемични мерки и да намалят риска от значително разпространение на вируса. Поради това те следва да бъдат важен елемент от стратегията за излизане от кризата в допълнение към други мерки, като например увеличаването на капацитета за изследване ([2]). Доверието е важна предпоставка за разработването на такива приложения и за приемането и използването им от хората. Хората трябва да имат увереността, че е гарантирано спазването на основните права и че мобилните приложения ще се използват само за специално определени цели, а не за масово наблюдение, както и че ползвателите им ще запазят контрола върху своите данни. От това зависят точността и ефективността на тези приложения при ограничаването на разпространението на вируса. Поради това е от основно значение е да се набележат решения, при

([1]) Препоръка C(2020) 2296 final от 8 април 2020 г. https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32020H0518&qid=1586975724070.

([2]) https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf.

които има възможно най-малко вмешателство и които отговарят напълно на изискванията относно защитата на личните данни и неприкосновеността на личния живот, определени в правото на ЕС. Освен това мобилните приложения следва да бъдат дезактивирани най-късно в момента, когато бъде обявено, че пандемията е под контрол. Те следва също така да включват най-съвременна защита на сигурността на информацията.

В настоящите насоки са взети предвид приносът на Европейския комитет по защита на данните ([3]) и обсъжданията в рамките на мрежата eHealth. Европейският комитет по защита на данните планира да публикува през следващите дни насоки относно геолокацията и други инструменти за проследяване в контекста на разпространението на COVID-19.

Обхват на насоките

За да се осигури последователен подход в целия ЕС и за да се предоставят насоки на държавите членки и разработчиците на мобилни приложения, в настоящия документ се посочват характеристиките и изискванията, на които приложенията следва да отговарят, за да се гарантира спазването на законодателството на ЕС в областта на неприкосновеността на личния живот и защитата на личните данни, и по-специално на Общия регламент относно защитата на данните (ОРЗД) ([4]) и Директивата за правото на неприкосновеност на личния живот и електронните комуникации ([5]). В настоящите насоки не се разглеждат никакви други условия, включително ограничения, които е възможно държавите членки да са включили в националните си законодателства по отношение на обработката на данни, свързани със здравето.

Насоките нямат правнообвързващ характер. Те не засягат ролята на Съда на ЕС, който е единствената институция, която може да даде официално тълкуване на правото на ЕС.

Настоящите насоки се отнасят само до доброволните мобилни приложения, които подпомагат борбата с пандемията от COVID-19 (т.е. които са изтеглени, инсталирани и използвани на доброволни начала от физически лица), разполагащи с една или повече от следните функции:

— предоставяне на лицата на точна информация за пандемията от COVID-19;

— предоставяне на лицата на въпросници за самооценка и за насоки (функция за проверка на симптомите) ([6]);

— известяване на лицата, които за определено време са се намирали в близост до заразено лице, за да им се предостави информация, като например дали да се поставят сами под карантина и къде да бъдат изследвани (функция за проследяване на контактите и за предупреждение);

— осигуряване на форум за комуникация между самоизолиралите се пациенти и лекари или за поставяне на допълнителна диагноза и предоставяне на съвети за лечение (по-голямо използване на телемедицина).

Съгласно Директивата за правото на неприкосновеност на личния живот и електронните комуникации налагането на задължение за използване на дадено мобилно приложение, засягащо правата на поверителност на комуникациите, посочени в член 5, е възможно единствено чрез закон, който е необходим, подходящ и пропорционален, за да се защитят определени конкретни цели. Предвид високата степен на вмешателство на такъв подход и свързаните с това предизвикателства, включително по отношение на въвеждането на подходящи гаранции, Комисията е на мнение, че е необходим внимателен анализ, преди да се използва този вариант. Поради тези причини Комисията препоръчва използването на доброволни мобилни приложения.

Настоящите насоки не обхващат мобилните приложения, имащи за цел изпълнение на изискванията за карантина (включително задължителните).

2 ПРИНОС НА МОБИЛНИТЕ ПРИЛОЖЕНИЯТА КЪМ БОРБАТА С COVID-19

Функцията за проверка на симптомите е средство, чрез което органите за обществено здравеопазване могат да предоставят на гражданите насоки за изследване за COVID-19 и информация за самоизолацията, за това как да се избегне предаването на вируса на други лица и кога да се потърсят здравни грижи. Тази функция може също така да допълни наблюдението на първичните здравни грижи и да спомогне за по-точно установяване на нивата на заразяване на населението с COVID-19.

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

([4]) 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 (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

([5]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронните комуникации) (ОВ L 201, 31.7.2002 г., стр. 37).

([6]) Ако мобилните приложения предоставят информация, свързана с диагностициране, превенция, наблюдение, предвиждане или прогнозиране, следва да се извърши оценка на потенциалното им квалифициране като медицински изделия в съответствие с нормативната рамка за медицинските изделия. За тази рамка — вж. Директива 93/42/ЕИО на Съвета от 14 юни 1993 г. относно медицинските изделия (ОВ L 169, 12.7.1993 г., стр. 1) и Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия (ОВ L 117, 5.5.2017 г., стр. 1).

Функциите за проследяване на контактите и за предупреждение са средства за идентифициране на хората, които са били в контакт с лице, заразено с COVID-19, и за информирането им за подходящите следващи стъпки, като например самопоставяне под карантина, изследване или предоставяне на съвети за това какво да се направи при наличие на симптоми. Ето защо тази функция е полезна както за физическите лица, така и за органите за обществено здравеопазване. Тя може също така да играе важна роля за овладяването на заразата при постепенна отмяна на противоепидемичните мерки. Ефектът от тази функция може да бъде подсилен чрез стратегия в подкрепа на по-мащабно изследване на хората с леки симптоми.

И двете функции могат също да бъдат съответен източник на данни за органите на общественото здравеопазване и да улесняват предаването на тези данни на националните епидемиологични органи и на Европейския център за профилактика и контрол върху заболяванията (ECDC). Това ще помогне за разбирането на моделите на предаване и, ако е съчетано с резултати от тестове, да бъде оценена положителната прогнозна стойност на респираторните симптоми в дадена общност, както и ще предостави информация за равнището на разпространение на вируса.

Степента на надеждност на оценките е пряко свързана с броя и надеждността на предадените данни.

Поради това, в комбинация със съответните стратегии за тестване, функциите за проверка на симптомите и проследяване на контактите могат предоставят информация относно степента на разпространение на вируса и могат да помогнат за оценката на въздействието на мерките за физическо дистанциране и изолация. Както се посочва в препоръката, за да е възможно трансграничното сътрудничество и за да се гарантира откриването на контакт между потребителите на различните приложения (което е особено важно при трансграничните движения на граждани) следва да се осигури оперативна съвместимост между ИТ решенията на различните държави членки. Когато заразено лице е в контакт с ползвател на мобилно приложение от друга държава членка, следва да е възможно личните данни на този ползвател да бъдат предадени трансгранично на здравните органи на неговата държава членка, доколкото това е строго необходимо. Работата по този въпрос ще се осъществи като част от набора от инструменти, обявен в препоръката. Оперативната съвместимост следва да бъде осигурена както чрез технически изисквания, така и чрез подобряване на комуникацията и сътрудничеството между националните здравни органи. Даден модел на конкретно сътрудничество ([7]) може да се използва също като модел за управление на мобилните приложения за проследяване на контакти по време на пандемията от COVID-19.

3 ЕЛЕМЕНТИ ЗА НАДЕЖДНО И ОТГОВОРНО ИЗПОЛЗВАНЕ НА МОБИЛНИТЕ ПРИЛОЖЕНИЯ

Функциите, включени в мобилните приложения, могат да имат различно въздействие върху широк кръг от права, залегнали в Хартата на основните права на ЕС, като човешкото достойнство, зачитането на личния и семейния живот, защитата на личните данни, свободата на движение, недискриминацията, свободата на стопанската инициатива и свободата на събрания и свободата на сдружаване. Вмешателствата в неприкосновеността на личния живот и правото на защита на личните данни могат да бъдат особено съществени, като се има предвид, че някои от функциите се основават на модел с интензивно използване на данни.

Представените по-долу елементи имат за цел да предоставят насоки за това как да бъде ограничено вмешателството на функциите на мобилното приложение, за да се гарантира спазването на законодателството на ЕС в областта на защитата на личните данни и неприкосновеността на личния живот.

3.1 Националните здравни органи (или субектите, които изпълняват задачи от обществен интерес в областта на здравеопазването) като администратори на данни

Определянето на това кой решава за средствата и целите на обработването на данните (администраторът на данни) е от решаващо значение, за да се установи кой отговаря за спазването на правилата на ЕС за защита на личните данни, и по-специално: кой следва да предостави информация на лицата, които изтеглят мобилното приложение относно това какво ще се случи с техните лични данни (вече съществуващи или които ще бъдат генерирани чрез устройство като смартфон, на което се инсталира мобилното приложение), какви ще бъдат техните права, кой ще бъде отговорен в случай на нарушаване на неприкосновеността на данните и др.

Като се има предвид чувствителността на разглежданите лични данни и целта на обработката на данните, описано по-долу, Комисията е на мнение, че мобилните приложения следва да бъдат замислени по такъв начин, че администратори на данните да бъдат националните здравни органи (или субектите, изпълняващи задачи от обществен интерес в областта на здравеопазването) ([8]). Администраторите отговарят за спазването на ОРЗД (принцип на отчетност). Обхватът на този достъп следва да бъде ограничен въз основа на принципите, описани в раздел 3.5 по-долу.

([7]) Това сътрудничество вече се осъществява по отношение на проекта MyHealth@EU за обмен на досиетата и електронните рецепти на пациентите. Вж. също член 5, параграф 5 и съображение 17 от Решение за изпълнение 2019/1765 на Комисията.

([8]) Вж. съображение 45 от ОРЗД.

Това ще допринесе и за по-голямото доверие сред населението, а оттук и за приемането на мобилните приложения (и свързаните с тях информационни системи относно веригите за предаване на инфекции) и ще гарантира, че те отговарят на предвиденото предназначение за защита на общественото здраве. Отговорните национални здравни органи трябва да съгласуват и прилагат по координиран начин съответните политики, изисквания и проверки.

3.2 **Гарантиране, че ползвателите запазват контрол**

Определящ фактор, за да имат ползвателите доверие в мобилните приложенията, е да им се докаже, че те запазват контрола върху личните си данни. За да се гарантира това, Комисията счита, че следва да бъдат изпълнени по-специално следните условия:

— инсталирането на мобилното приложение на тяхното устройство следва да бъде доброволно и без никакви отрицателни последици за лицето, което решава да не изтегля/използва приложението;

— различните функции на мобилното приложение (напр. информационните, за проверка на симптомите, проследяване на контактите и предупреждение) следва да не бъдат групирани, така че лицето да може да даде конкретното си съгласието за всяка една от тях. Това не следва да пречи на ползвателя да комбинира различни функции на приложението, ако доставчикът предлага тази възможност;

— ако се използват данни за хора и обекти в непосредствена близост (данни, генерирани от обмена на сигнали чрез Bluetooth Low Energy (BLE) между устройства, които се намират на епидемиологично значимо разстояние и в епидемиологично значим момент), те следва да се съхраняват върху устройството на лицето. Ако тези данни трябва да бъдат споделени със здравните органи, те следва да се споделят само след като бъде потвърдено, че засегнатото лице е заразено с COVID-19, и при условие че то реши да направи това;

— здравните органи следва да предоставят на лицето цялата необходима информация, свързана с обработването на неговите лични данни (в съответствие с членове 12 и 13 от ОРЗД и член 5 от Директивата за правото на неприкосновеност на личния живот);

— лицето следва да може да упражнява правата си съгласно ОРЗД (по-специално, за достъп, коригиране, заличаване). Всяко ограничаване на правата съгласно ОРЗД и Директивата за правото на неприкосновеност на личния живот следва да бъде в съответствие с тези актове и да бъде необходимо, пропорционално и предвидено в законодателството;

— мобилните приложения следва да бъдат дезактивирани най-късно, когато бъде обявено, че пандемията е под контрол; дезактивирането не следва да зависи от това ползвателят сам да деинсталира приложението.

3.3 **Правно основание за обработването**

Инсталиране на мобилните приложения и съхраняване на информация върху устройството на ползвателя

Както е отбелязано по-горе, съгласно Директивата за правото на неприкосновеност на личния живот (член 5) съхраняването на информация върху устройството на ползвателя или получаването на достъп до вече съхранената информация се допуска само ако i) ползвателят е дал съгласието си или ii) съхранението и/или достъпът е строго необходим за услугата на информационното общество (например приложението), изрично поискана (т.е. инсталирана и активирана) от ползвателя.

Съхраняването на информацията върху устройството на лицето и получаването на достъп до информацията, която вече се съхранява на това устройство, обикновено са необходими за функционирането на мобилните приложения. Освен това за функцията за проследяване на контакти и предупреждение е необходимо върху устройството на потребителя да бъде съхранявана друга информация (като например краткотрайни, периодично променящи се псевдонимни идентификатори на ползвателите на тази функция, намиращи се в непосредствена близост). Освен това за тази функция може да е необходимо (заразеният или вероятно заразен) ползвател да качва данни за хора и обекти в непосредствена близост. Това качване не е необходимо за функционирането на самото приложение. Поради това не са спазени изискванията за вариант ii), посочени в предходния параграф. По тази причина вариантът със съгласието (i) по-горе) остава най-подходящото основание за съответните дейности. Това съгласие следва да бъде „свободно изразено“, „конкретно“, „изрично“ и „информирано“ по смисъла на ОРЗД. То следва да бъде изразено чрез ясно утвърдително действие от страна на лицето; това изключва мълчаливите форми на съгласие (например мълчание; бездействие) ([9]).

([9]) Вж. насоките на Европейския комитет по защита на данните относно съгласието: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Правно основание за обработването от националните здравни органи — право на Съюза или на държава членка

Националните здравни органи обикновено обработват лични данни, когато в правото на ЕС или на държавата членка се съдържа правно задължение, предвиждащо такова обработване и отговарящо на условията по член 6, параграф 1, буква в) и член 9, параграф 2, буква и) от ОРЗД, или когато това обработване е необходимо за изпълнението на задача за засилване на обществения интерес, призната от правото на ЕС или правото на държава членка ([10]).

Националното законодателство трябва да предвижда конкретни и подходящи мерки за защита на правата и свободите на субектите на данни. Като общо правило, колкото по-голямо е въздействието върху свободите на лицата, толкова по-строги съответни гаранции следва да бъдат предвидени в съответното законодателство.

Законите на ЕС и на държавите членки, които са били в сила преди разпространението на COVID-19, и тези, които са били приети в държавите членки специално за борба с разпространението на епидемии, могат по принцип да се използват като правно основание за обработването на данните на лицата, ако в тях се предвиждат мерки, позволяващи мониторинг на епидемиите, и ако тези закони отговарят на допълнителните изисквания, определени в член 6, параграф 3 от ОРЗД.

Като се има предвид естеството на съответните лични данни (по-специално здравни данни като специални категории лични данни), както и обстоятелствата около настоящата пандемия от COVID- 19, да се разчита на закона като правно основание, би допринесло за правна сигурност, тъй като законът: i) би предписал подробно обработването на специфични здравни данни и би уточнил ясно целите на обработването; ii) би посочил ясно кой е администраторът на данните, т.е. субектът, обработващ данните, и кой освен администратора може да има достъп до тези данни; iii) би изключил възможността за обработване на такива данни за цели, различни от изброените в законодателството, и iv) би предвидил конкретни гаранции. За да не се наруши обществената полза и приемането на мобилните приложения от обществеността, националният законодател следва да внимава специално за това избраното решение да е възможно най-приобщаващо по отношение на гражданите.

Обработването от страна на здравните органи въз основа на законодателството не променя факта, че физическите лица са свободни да инсталират мобилното приложение или не и да споделят данните си със здравните органи. Поради това, когато мобилното приложение не е инсталирано, това не следва да води до неблагоприятни последици за потребителите.

Мобилните приложения за проследяване на контактите и за предупреждение осигуряват предупреждаването на физическите лица. Когато това предупреждение е осигурено пряко от мобилното приложение, Комисията обръща внимание на забраната да се подлагат лицата на решение, основаващо се единствено на автоматизирано обработване, което поражда правни последици или по подобен начин ги засяга в значителна степен (член 22 от ОРЗД).

3.4 **Свеждане на данните до минимум**

Получените чрез устройствата данни и вече съхранявани в тези устройства преди това са защитени, както следва:

— Като „лични данни“, т.е. всяка информация, свързана с идентифицирано или подлежащо на идентифициране физическо лице (член 4, параграф 1 от ОРЗД), те са защитени по ОРЗД. Данните за здравословното състояние се ползват с допълнителна защита (член 9 от ОРЗД).

— Като „данни за местоположението“, т.е. данни, обработени в електронна съобщителна мрежа или чрез електронна съобщителна услуга, указващи географското местоположение на крайното оборудване на ползвателя, са защитени по силата на Директивата за правото на неприкосновеност на личния живот и електронни комуникации (член 5, параграф 1, членове 6 и 9) ([11]),

— Всяка информация, съхранявана в крайното оборудване на ползвателя, и до която се осъществява достъп от това оборудване, е защитена съгласно член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

Неличните данни (като например необратимо анонимизираните данни) не са защитени съгласно ОРЗД.

Комисията припомня, че принципът за свеждане на данните до минимум изисква да могат да се обработват само лични данни, които са адекватни, уместни и ограничени до необходимото за целта ([12]). Оценка на необходимостта от обработване на личните данни и на уместния характер на тези лични данни следва да се извършва с оглед на преследваната(ите) цел(и).

Комисията отбелязва, че например, ако целта на функцията е проверка на симптомите или телемедицина, за тези цели не се изисква достъп до списъка с данни за контакт на лицето, което притежава устройството.

([10]) Член 6, параграф 1, буква д) от ОРЗД.

([11]) В Кодекса за електронните съобщения се предвижда, че неговият обхват включва и услугите, които са функционално равностойни на електронните съобщителни услуги.

([12]) Принцип на свеждане на данните до минимум

Генерирането и обработването на по-малко данни ограничават рисковете за сигурността. Поради това спазването на мерките за свеждане на данните до минимум осигурява и гаранции за сигурността.

— Информационна функция:

Мобилно приложение само с тази функция няма нужда да обработва здравни данни на физически лица. То просто ще им предостави информация. За да се изпълни тази цел, не може да се обработва информация, съхранявана в крайното оборудване на ползвателя, и до която се осъществява достъп от това оборудване, различна от необходимото за предоставяне на информацията.

— Функции за проверка на симптомите и за телемедицина:

Ако мобилното приложение включва една или две от тези функции, то ще обработва лични здравни данни. Поради това в приложимото законодателство за здравните органи следва да бъде посочен списък с данни, които могат да бъдат обработвани.

Освен това здравните органи могат да се нуждаят от телефонните номера на лицата, които са използвали проверката на симптомите и са качили резултатите. Информацията, информация, съхранявана в крайното оборудване на ползвателя, и до която се осъществява достъп от това оборудване, може да се обработва само дотолкова, доколкото това е необходимо, за да може приложението да изпълнява своята цел и да функционира.

— Функция за проследяване на контактите и предупреждение:

По-голямата част от инфекциите с COVID-19 се извършват чрез капчици, които изминават само ограничено разстояние. Възможно най-бързото идентифициране на лицата, които са били в близост до заразено лице, е ключов фактор за прекъсване на веригата на заразяване. Установяването на близостта е функция от разстоянието и продължителността на контакта и следва да се извършва от епидемиологична гледна точка. Прекъсването на веригата на заразяване е от особено значение, за да се избегне възобновяване на инфекциите на етапа на излизане от кризата.

За тази цел може да са необходими данни за хора и обекти в непосредствена близост. За измерване на близостта и тесните контакти технологията Bluetooth Low Energy (BLE) за контакти между устройствата изглежда по-точна и следователно по-подходяща от използването на данни за географското позициониране (GNSS/GPS или данни за местоположението на клетките). BLE избягва възможността за проследяване (обратно на данните за географското позициониране). Поради това Комисията препоръчва използването на данни от съобщенията BLE (или данни, генерирани от еквивалентни технологии), за да се определи близостта.

Данните за местоположението не са необходими за целите на функциите за проследяване на контактите, тъй като тяхната цел не е проследяване на движението на лица или прилагане на предписания. Освен това обработването на данни за местоположението в контекста на проследяването на контактите би било трудно за обосноваване с оглед на принципа за свеждане до минимум на данните и може да създаде проблеми по отношение на сигурността и неприкосновеността на личния живот. Поради тази причина Комисията препоръчва в този контекст да не се използват данни за местоположението.

Независимо от използваните технически средства за определяне на близостта, не е необходимо да се съхранява информация за точния момент на контакта или за мястото на осъществяването му (ако е налице). Въпреки това може да е от полза да се съхранява денят на осъществяване на контакта, за да се знае дали контактът е бил осъществен, когато лицето е проявило симптоми (или 48 часа преди това ([13])), и да се дадат насоки за последващото съобщение със съвети за това колко дълго време да се подложи само на карантина.

Данните за хора и обекти в непосредствена близост следва да се генерират и обработват само ако съществува реален риск от заразяване (в зависимост от близостта и продължителността на контакта).

Следва да се отбележи, че поради това необходимостта и пропорционалността на събирането на данни ще зависят от фактори, като например степента, до която са налични съоръжения за тестване, по-специално когато вече са били постановени мерки за изолация. Предупреждаването на лица, които са били в близък контакт със заразено лице, може да бъде направено по два начина:

Съгласно първия подход се подава автоматично сигнал за предупреждение чрез приложението към лицата, които са били в близък контакт, когато ползвател изпрати уведомление в приложението — с одобрението или потвърждението от здравния орган, например чрез код QR или TAN — че ползвателят е с положителен резултат от тест (децентрализирана обработка). Препоръчително е съдържанието на съобщението за предупреждение да бъде определено от здравния орган. При втория подход произволните временни идентификатори се съхраняват на бекенд сървър на здравния орган (решение с бекенд сървър). Ползвателите не могат да бъдат пряко идентифицирани чрез тези данни. Чрез идентификаторите ползвателите, които са били в близък контакт с ползвател с положителен резултат от тест, получават предупреждение на устройството си. Ако здравните органи желаят да се свържат с ползвателите, които са били в тесен контакт със заразено лице и чрез телефон или SMS, те се нуждаят от съгласието на тези ползватели да предоставят телефонните си номера.

([13]) Инфектираното лице е заразно 48 часа преди появата на симптомите.

3.5 **Ограничаване на оповестяването/достъпа до данни**

— Информационна функция:

Никаква информация, съхранявана в крайното оборудване, и до която се осъществява достъп от това оборудване, не може да бъде споделяна със здравните органи, освен тази, която е необходима, за да се поддържа информационната функция. Тъй като тази функция предвижда само средствата за комуникация, здравният орган няма да получи достъп до никакви други данни.

— Функции за проверка на симптомите и за телемедицина:

Функцията за проверка на симптомите може да е от полза за държавите членки, за да насочват гражданите относно това дали трябва да бъдат тествани, да предоставят информация за изолацията и за това кога и как да се получи достъп до здравно обслужване, особено за рисковите групи. Тази функция може също така да допълни наблюдението на първичните здравни грижи и да спомогне да се установи какви са нивата на заразяване с COVID-19 на населението. Поради това може да бъде решено, че отговорните здравни органи и националните епидемиологични органи следва да получат достъп до информацията, предоставена от пациента. ECDC може да получава обобщени данни от националните органи за епидемиологично наблюдение.

Ако се избере да се даде възможност за контакт със здравни служители, а не само чрез самото приложение, след това е необходимо също да се съобщят на националните здравни органи телефонните номера на ползвателите на мобилните приложения.

— Функция за проследяване на контактите и предупреждаване:

— Данни за заразеното лице

Приложенията генерират псевдослучайни краткотрайни и периодично променящи се идентификатори на телефоните, които са в контакт с потребителя. Един от вариантите е идентификаторите да бъдат съхранявани на устройството на потребителя (т. нар. децентрализирана обработка). Друг вариант може да предвижда тези произволни идентификатори да се съхраняват на сървъра, до който имат достъп здравните органи (т.нар. решение, основаващо се на бекенд сървър). Децентрализираното решение съответства в по-голяма степен на принципа на свеждане на данните до минимум. Достъпът на здравните органи до данни от устройството на заразено лице следва да бъде ограничен само до данни за хора и обекти в непосредствена близост, така че здравните органи да бъдат в състояние да се свържат с хора, изложени на риск от инфекция.

Тези данни ще бъдат на разположение на здравните органи едва след като заразеното лице (след като е било подложено на тест) проактивно ги сподели с тях.

Заразеното лице не следва да получава информация за самоличността на лицата, с които е било в контакт от потенциално епидемиологично значение и които ще бъдат предупредени.

— Данни на лицата, които са били в (епидемиологичен) контакт със заразеното лице

Самоличността на заразеното лице не следва да бъде разкривана на лицата, с които то е било в епидемиологичен контакт. Достатъчно е да им се съобщи фактът, че през последните 16 дни са били в епидемиологичен контакт със заразено лице. Както е посочено по-горе, не следва да се съхраняват данни за времето и мястото на такива контакти. Следователно предаването на такива данни нито е необходимо, нито е възможно.

За проследяване на епидемиологичните контакти на потребител на приложението, за когото е установено, че е заразен, националните здравни органи следва да бъдат информирани само за идентификатора на лицето, с което заразеното лице е било в епидемиологичен контакт най-рано 48 часа преди началото на симптомите и най-късно 14 дни след това, въз основа на близостта и продължителността на контакта.

ECDC може да получава обобщени данни за проследяване на контактите от националните органи за епидемиологично наблюдение по показатели, определени в сътрудничество с държавите членки.

3.6 **Определяне на конкретните цели на обработването**

Правното основание (правото на Съюза или правото на държава членка) следва да урежда целта на обработването. Целта следва да бъде конкретна и изрична, така че да няма съмнение относно това какъв вид лични данни е необходимо да бъдат обработвани, за да се постигне желаният резултат.

Точната цел(и) ще зависи(ят) от функциите на приложението. Може да има няколко цели за всяка функция на дадено приложение. За да предостави на лицата пълен контрол върху техните данни, Комисията препоръчва да не се обединяват различни функции. Във всеки случай лицето следва да има възможност да избира между различни функции, всяка от които преследва отделна цел.

Комисията препоръчва да не се използват данните, събрани при горепосочените условия, за други цели, различни от борбата срещу COVID-19. Ако са необходими научни изследвания и статистически данни, тези цели следва да бъдат включени в първоначалния списък с цели и да бъдат ясно съобщени на потребителите.

— Информационна функция:

Целта на тази функция е предоставянето на информация от значение за здравните органи в контекста на кризата.

— Функции за проверка на симптомите и за телемедицина:

Функцията за проверка на симптомите може да даде представа за това каква част от лицата, които съобщават за симптоми, съответстващи на заболяване от COVID-19, действително са заразени (например чрез вземане на натривка и тестване на всички или на произволен брой лица с такива симптоми, ако има възможност за това). При така определената цел трябва ясно да се посочи, че личните здравни данни ще бъдат обработвани с цел: i) да се даде възможност на ползвателя да оцени самостоятелно, въз основа на набор от въпроси, дали е проявил симптоми на COVID-19, или ii) да потърси медицински съвет, ако е проявил симптоми на COVID-19.

— Функции за проследяване на контактите и предупреждаване:

Простото посочване на цел „предотвратяване на по-нататъшно заразяване с COVID-19“ не е достатъчно конкретно. В този случай Комисията препоръчва допълнително уточняване на целта(ите) в следната насока: „запазване на данни за лицата, които са били в контакт с ползватели на приложението и които може да са били изложени на инфекция с COVID-19, с цел да бъдат предупредени потенциално заразените лица“.

3.7 **Определяне на строги ограничения за съхранението на данните**

Принципът на ограничение на съхранението изисква личните данни да не се съхраняват по-дълго от необходимото. Сроковете следва да се основават на медицинската значимост на данните (в зависимост от целта на приложението: инкубационен период и др.), както и на реалистичното време за извършването на административните действия, които може да бъдат необходими.

— Информационна функция:

В случай че се събират данни при инсталирането на тази функция, те следва да бъдат незабавно изтрити. Няма основание за съхраняването на такива данни.

— Функции за проверка на симптомите и за телемедицина:

Тези данни следва да бъдат изтрити от здравните органи в срок до един месец (инкубационен период плюс допълнителен марж) или след като лицето е било тествано и резултатът е отрицателен. Здравните органи може да съхраняват данни за по-дълги периоди от време с цел докладване на извършеното наблюдение и научни изследвания, при условие че данните са в анонимна форма.

— Функции за проследяване на контактите и предупреждаване:

Данните за хора и обекти в непосредствена близост следва да бъдат заличени веднага след като престанат да бъдат необходими за целите на предупреждаването. Такъв би бил случаят след максимум един месец (инкубационен период плюс марж) или след като лицето е било тествано и резултатът е отрицателен. Здравните органи може да съхраняват данни за хора и обекти в непосредствена близост за по-дълги периоди от време с цел докладване на извършеното наблюдение и научни изследвания, при условие че данните са в анонимна форма.

Данните следва да се съхраняват в устройството на ползвателя и само данните, които са съобщени от ползвателите и са необходими за изпълнение на целта, следва да бъдат качени на сървъра на разположение на здравните органи, когато е избрана тази опция (например качване на сървъра само на данни за лица, които са в „близък контакт“ с лице, което е показало положителен резултат за инфекция с COVID-19).

3.8 **Гарантиране на сигурността на данните**

Комисията препоръчва данните да се съхраняват върху крайното устройство на лицето в криптирана форма, като се използват най-съвременни криптографски техники. В случай че данните се съхраняват на централен сървър, следва да се регистрира достъпът, включително административният достъп.

Данните за хора и обекти в непосредствена близост следва да се генерират и съхраняват само на крайното устройство на лицето в криптиран и псевдонимизиран формат. С цел да се гарантира, че проследяването от трети страни е изключено, активирането на Bluetooth следва да бъде възможно, без да е необходимо да се активират други услуги за установяване на местоположението.

По време на събирането на данни за хора и обекти в непосредствена близост чрез BLE е за предпочитане да се създават и съхраняват временни потребителски идентификатори, които често се променят, вместо да се съхранява действителният идентификатор на устройството. Тази мярка осигурява допълнителна защита срещу подслушване и проследяване от хакери и поради това затруднява идентифицирането на лицата.

Комисията препоръчва изходният код на приложението да бъде оповестен публично и да бъде на разположение за преглед.

Може да се предвидят допълнителни мерки за гарантиране на сигурността на обработваните данни, по-специално чрез автоматично заличаване или анонимизиране на данните след определен период от време. Като цяло степента на сигурност следва да съответства на количеството и чувствителността на обработваните лични данни.

Всички данни, предавани от личното устройство до националните здравни органи, следва да бъдат криптирани.

Когато националното законодателство допуска по-нататъшно обработване на събраните лични данни за целите на научни изследвания, следва по принцип да се използва псевдонимизация.

3.9 **Гарантиране на точността на данните**

Гарантирането на точността на обработваните лични данни е не само предпоставка за ефективността на приложението, но е и изискване съгласно законодателството за защита на личните данни.

В този контекст, за да се сведе до минимум рискът от фалшиви положителни резултати, от съществено значение е да се гарантира точността на информацията относно това дали е налице контакт със заразеното лице (епидемиологична отдалеченост и продължителност). Това следва да включва сценарии, при които двама ползватели на приложението са в контакт на улицата, в обществения транспорт или в сграда. Малко вероятно е използването на данни за местоположението въз основа на мобилни мрежи да е достатъчно точно за тази цел.

Поради това е препоръчително да се използват технологии, позволяващи по-точна оценка на контактите (като например Bluetooth).

3.10 **Участие на органите за защита на данните**

Органите за защита на данните следва да участват пълноценно и да бъдат консултирани в контекста на разработването на приложението и да наблюдават въвеждането му. Като се има предвид, че обработването на данни в контекста на приложението ще попадне в приложното поле на понятието мащабно обработване на специални категории лични данни (здравни данни), Комисията обръща внимание на член 35 от ОРЗД относно оценката на въздействието върху защитата на данните.

ISSN 1977-0855 (електронно издание)
ISSN 1830-365X (печатно издание)



Служба за публикации на Европейския съюз
2985 Люксембург
ЛЮКСЕМБУРГ

BG