II

(Незаконодателни актове)

РЕШЕНИЯ

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2020/1023 НА КОМИСИЯТА

от 15 юли 2020 година

за изменение на Решение за изпълнение (ЕС) 2019/1765 по отношение на трансграничния обмен на данни между националните мобилни приложения за проследяване на контактите и за предупреждаване в рамките на борбата с пандемията от COVID-19

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Директива 2011/24/ЕС на Европейския парламент и на Съвета от 9 март 2011 г. за упражняване на правата на пациентите при трансгранично здравно обслужване ([1]), и по-специално член 14, параграф 3 от нея,

като има предвид, че:

(1) По силата на член 14 от Директива 2011/24/ЕС Съюзът има за задача да подкрепя и улеснява сътрудничеството и обмена на информация между държавите членки, работещи в рамките на мрежа, изградена на доброволна основа и свързваща определените от държавите членки национални органи, отговарящи за електронното здравеопазване („мрежата за електронно здравеопазване“).

(2) В Решение за изпълнение (ЕС) 2019/1765 на Комисията ([2]) са предвидени правилата за учредяването, управлението и функционирането на мрежата от национални органи, отговарящи за електронното здравеопазване, По силата на член 4 от посоченото решение на мрежата за електронно здравеопазване е поверена задачата да допринася за по-голяма оперативна съвместимост на националните системи за информационни и комуникационни технологии и за трансграничната преносимост на електронните данни за здравословното състояние при трансгранично здравно обслужване.

(3) В контекста на кризата с общественото здраве, причинена от пандемията от COVID-19, държавите членки разработиха мобилни приложения, които подпомагат проследяването на контактите и дават възможност на потребителите на такива приложения да бъдат предупреждавани с оглед предприемането на подходящи действия, като например тестване или самоизолиране, ако евентуално са били изложени на вируса в непосредствена близост до друг потребител на такива приложения, който е дал положителен резултат при тестване. Тези приложения се основават на Bluetooth технологията с цел откриване на близки контакти между различни устройства. Тъй като ограниченията за пътуванията между държавите членки бяха премахнати от юни 2020 г. насам, следва да се постигне по-голяма оперативна съвместимост на националните системи за информационни и комуникационни технологии между държавите членки, участващи в мрежата за електронно здравеопазване, чрез изграждане на цифрова инфраструктура, даваща възможност за оперативна съвместимост между националните мобилни приложения, подпомагащи проследяването на контактите и предупреждаването.

([1]) ОВ L 88, 4.4.2011 г., стр. 45.

([2]) Решение за изпълнение (ЕС) 2019/1765 на Комисията от 22 октомври 2019 г. за предвиждане на правила за учредяването, управлението и функционирането на мрежата от национални органи, отговарящи за електронното здравеопазване, и за отмяна на Решение за изпълнение 2011/890/ЕС (ОВ L 270, 24.10.2019 г., стр. 83).

(4) Комисията оказва подкрепа на държавите членки във връзка с посочените по-горе мобилни приложения. 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-долу „Препоръката на Комисията“) ([3]). Държавите членки, участващи в мрежата за електронно здравеопазване, приеха с подкрепата на Комисията общ инструментариум на ЕС за държавите членки относно мобилните приложения, подпомагащи проследяването на контактите ([4]), както и насоки за оперативна съвместимост за одобрените мобилни приложения за проследяване на контакти в ЕС ([5]). В инструментариума са разяснени националните изисквания във връзка с националните мобилни приложения за проследяване на контактите и предупреждаване, като по-специално се уточнява, че същите следва да се използват на доброволна основа, да са одобрени от компетентния национален орган по въпросите на здравеопазването, да осигуряват зачитане на неприкосновеността на личния живот и да бъдат премахвани, веднага щом отпадне необходимостта от тях. След последното развитие на кризата с COVID-19 Комисията ([6]) и Европейският комитет по защита на данните ([7]) издадоха поотделно указания във връзка със защитата на данните в рамките на мобилните приложения и инструментите за проследяване на контактите. Разработването на мобилните приложения на държавите членки и на цифровата инфраструктура, която позволява тяхната оперативна съвместимост, се основава на общия инструментариум на ЕС, на посочените по-горе насоки и на техническите спецификации, договорени в рамките на мрежата за електронно здравеопазване.

(5) За да се спомогне за оперативната съвместимост на националните мобилни приложения за проследяване на контактите и предупреждаване, държавите членки, участващи в мрежата за електронно здравеопазване, които решиха да задълбочат на доброволна основа сътрудничеството помежду си в тази област, разработиха с подкрепата на Комисията цифрова инфраструктура под формата на ИТ инструмент за обмен на данни. Тази цифрова инфраструктура е наречена „федерираният портал“.

(6) Настоящото решение съдържа разпоредби относно ролята на участващите държави членки и на Комисията във връзка с функционирането на федерирания портал за целите на трансграничната оперативна съвместимост на националните мобилни приложения за проследяване на контактите и предупреждаване.

(7) Обработката на личните данни на потребителите на мобилни приложения за проследяване на контактите и предупреждаване, за която носят отговорност държавите членки или други публични организации или официални органи в държавите членки, следва да се извършва в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([8]) („Общия регламент относно защитата на данните“) и Директива 2002/58/ЕО на Европейския парламент и на Съвета ([9]). Обработката на личните данни, за която носи отговорност Комисията, за целите на управлението и гарантирането на сигурността на федерирания портал следва да се извършва в съответствие с Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([10]).

(8) Федерираният портал следва да бъде под формата на защитена ИТ инфраструктура, осигуряваща общ интерфейс, посредством който определените национални или официални органи да могат да обменят минимален набор от данни във връзка с контактите с лица, заразени със SARS-CoV-2, за да информират останалите за евентуалната им експозиция на тази инфекция, и стимулираща чрез улесняване на обмена на релевантна информация ефикасното сътрудничество между държавите членки в областта на здравното обслужване.

(9) Поради това в настоящото решение следва да се определят редът и условията за трансграничен обмен на данни между определените национални или официални органи посредством федерирания портал в рамките на ЕС.

([3]) Препоръка (ЕС) 2020/518 на Комисията от 8 април 2020 г. 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 (ОВ L 114, 14.4.2020 г., стр. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Съобщение на Комисията, озаглавено „Насоки за мобилните приложения, които подпомагат борбата с пандемията от COVID-19, във връзка със защитата на данните“ (ОВ C 124I, 17.4.2020 г., стр. 1).

([7]) Насоки № 4/2020 относно използването на данни за местоположение и инструменти за проследяване на контакти в контекста на пандемията от COVID-19 и Изявление на Европейския комитет по защита на данните от 16 юни 2020 г. относно въздействието на оперативната съвместимост на приложенията за проследяване на контактите върху защитата на данните, като и двете са достъпни на следния адрес: https://edpb.europa.eu

([8]) 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).

([9]) 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 електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37).

([10]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39).

(10) Участващите държави членки, представлявани от определените национални или официални органи, заедно определят целта и средствата за обработване на лични данни посредством федерирания портал и поради това изпълняват ролята на съвместни администратори. В член 26 от Общия регламент относно защитата на данните се предвижда задължение за съвместните администратори на операции по обработване на лични данни да определят по прозрачен начин съответните си отговорности за изпълнение на задълженията по посочения регламент. В него също така се предвижда възможността тези отговорности да са определени от правото на Съюза или правото на държава членка, което е приложимо спрямо администраторите. Всеки от администраторите следва да гарантира, че разполага с правно основание на национално равнище за обработването на данни в рамките на федерирания портал.

(11) Комисията, в качеството си на доставчик на технически и организационни решения за федерирания портал, обработва псевдонимизирани лични данни от името на участващите в рамките на федерирания портал като съвместни администратори държави членки и поради това е обработващ лични данни. По силата на член 28 от Общия регламент относно защитата на данните и член 29 от Регламент (ЕС) 2018/1725 обработването от страна на обработващия лични данни се урежда с договор или с правен акт съгласно правото на Съюза или правото на държава членка, който е задължителен за обработващия лични данни спрямо администратора и който уточнява самата обработка. С настоящото решение се определят правилата за обработка от Комисията в качеството ѝ на обработващ лични данни.

(12) При обработването на лични данни в рамките на федерирания портал Комисията е обвързана от Решение (ЕС, Евратом) 2017/46 на Комисията ([11]).

(13) Предвид това, че целите, за които администраторите обработват лични данни в рамките на националните мобилни приложения за проследяване на контактите и предупреждаване, не изискват непременно идентифициране на отделния субект на данни, възможно е администраторите невинаги да са в състояние да гарантират прилагането на правата на субектите на данни. Поради това правата, посочени в членове 15—20 от Общия регламент относно защитата на данните, може да не се прилагат, когато са изпълнени условията по член 11 от същия регламент.

(14) Съществуващото приложение към Решение за изпълнение (ЕС) 2019/1765 е необходимо да бъде преномерирано поради добавянето на две нови приложения.

(15) Поради това Решение за изпълнение (ЕС) 2019/1765 следва да бъде съответно изменено.

(16) Предвид неотложния характер на ситуацията, породена от пандемията от COVID-19, настоящото решение следва да се прилага от деня след деня на публикуването му в *Официален вестник на Европейския съюз*.

(17) В съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 беше проведена консултация с Европейския надзорен орган по защита на данните, който на 9 юли 2020 г. излезе със становище.

(18) Мерките, предвидени в настоящото решение, са съобразени със становището на комитета, създаден съгласно член 16 от Директива 2011/24/ЕС,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Решение за изпълнение (ЕС) 2019/1765 се изменя, както следва:

1) В член 2, параграф 1 се добавят следните букви ж), з), и), й), к), л), м), н) и о):

„ж) „потребител на приложение“ означава притежаващо интелигентно устройство лице, което е изтеглило и използва одобрено мобилно приложение за проследяване на контактите и предупреждаване;

з) „проследяване на контакти“ означава мерки, изпълнявани с цел проследяване на лицата, които са били изложени на източник на сериозна трансгранична заплаха за здравето, по смисъла на член 3, буква в) от Решение № 1082/2013/ЕС на Европейския парламент и на Съвета (*);

([11]) Решение (ЕС, Евратом) 2017/46 на Комисията от 10 януари 2017 г. относно сигурността на комуникационните и информационните системи в Европейската комисия (ОВ L 6, 11.1.2017 г., стр. 40). Комисията публикува допълнителна информация за стандартите за сигурност, които се прилагат за всички информационни системи на Европейската комисия, на следната страница в Интернет: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en

и) „национално мобилно приложение за проследяване на контактите и предупреждаване“ означава одобрено на национално равнище софтуерно приложение, функциониращо върху интелигентни устройства, най-вече смартфони, в общия случай разработено за широкообхватно и целенасочено взаимодействие с уеб ресурси, което обработва данни и друга контекстуална информация, събирана от множество датчици, намиращи се в интелигентните устройства, за целите на проследяването на контактите в непосредствена близост с лица, заразени със SARS-CoV-2, и предупреждаване на лицата, които може да са били изложени на SARS-CoV-2. Тези мобилни приложения могат да откриват присъствието на други устройства, използващи Bluetooth технологията, и да обменят информация с бекенд сървъри чрез използване на интернет;

й) „федериран портал“ означава мрежов портал, управляван от Комисията чрез защитен ИТ инструмент, който получава, съхранява и предоставя минимален набор от лични данни между бекенд сървърите на държавите членки с цел да се гарантира оперативната съвместимост на националните мобилни приложения за проследяване на контактите и предупреждаване;

к) „ключ“ означава уникален ефимерен идентификатор, свързан с потребител на приложение, който съобщава, че е бил заразен със SARS-CoV-2, или който може да е бил изложен на SARS-CoV-2;

л) „верифициране на инфекция“ означава метод, прилаган за потвърждаване на заразяване със SARS-CoV-2, било то когато то е било съобщено от потребителя на приложението или е вследствие потвърждение от национален здравен орган или от лабораторно изследване;

м) „държави, представляващи интерес“ означава държавата членка или държавите членки, в която/които потребителят на приложението се е намирал през 14-те дни, предхождащи датата на качване на ключовете, и където е изтеглил одобреното национално мобилно приложение за проследяване на контактите и предупреждаване и/или е пътувал;

н) „държава на произход на ключовете“ означава държавата членка, в която се намира бекенд сървърът, качил ключовете във федерирания портал;

о) „журнални данни“ означава автоматичен запис на дейност, свързана с обмена на данни, обработвани посредством федерирания портал, а също и с достъпа до такива данни, който посочва по-специално вида на дейността по обработване, датата и времетраенето на дейността по обработване, както и идентификатора на лицето, обработващо данните.

_____

(*) Решение № 1082/2013/ЕС на Европейския парламент и на Съвета от 22 октомври 2013 г. за сериозните трансгранични заплахи за здравето и за отмяна на Решение № 2119/98/ЕО (ОВ L 293, 5.11.2013 г., стр. 1).“

2) В член 4, параграф 1 се добавя следната буква з):

„з) дава указания на държавите членки във връзка с трансграничния обмен на лични данни посредством федерирания портал между националните мобилни приложения за проследяване на контактите и предупреждаване.“

3) В член 6, параграф 1 се добавят следните букви е) и ж):

„е) разработва, прилага и поддържа необходимите технически и организационни мерки във връзка със сигурността на предаването и хостването на лични данни във федерирания портал с цел да се гарантира оперативната съвместимост на националните мобилни приложения за проследяване на контактите и предупреждаване;

ж) подпомага мрежата за електронно здравеопазване при одобряване на техническото и организационното спазване от националните органи на изискванията за трансграничния обмен на лични данни в рамките на федерирания портал, като организира и провежда необходимите тестове и одити. Експерти от държавите членки може да подпомагат одиторите на Комисията.“

4) Член 7 се изменя, както следва:

а) заглавието се заменя със „Защита на личните данни, обработвани посредством инфраструктурата за цифрови услуги в областта на електронното здравеопазване“;

б) в параграф 2 думата „приложението“ се заменя с израза „приложение I“.

5) Вмъква се следният член 7а:

„*Член 7а*

Трансграничен обмен на данни между националните мобилни приложения за проследяване на контактите и предупреждаване посредством федерирания портал

1. Когато се обменят лични данни посредством федерирания портал, обработването се ограничава до целите за улесняване на оперативната съвместимост на националните мобилни приложения за проследяване на контактите и предупреждаване в рамките на федерирания портал и за непрекъснатост на проследяването на контактите в трансграничен контекст.

2. Посочените в параграф 3 лични данни постъпват във федерирания портал в псевдонимизиран формат.

3. Псевдонимизираните лични данни, обменяни посредством федерирания портал и обработвани в него, включват единствено следната информация:

а) ключовете, предадени от националните мобилни приложения за проследяване на контактите и предупреждаване до 14 дни преди датата на качване на ключовете;

б) свързаните с ключовете журнални данни в съответствие с протокола за техническите спецификации, използван в държавата на произход на ключовете;

в) верифицирането на инфекцията;

г) държавите, представляващи интерес, и държавата на произход на ключовете.

4. Определените национални или официални органи, които обработват лични данни в рамките на федерирания портал, са съвместни администратори на данните, обработвани в този портал. Съответните отговорности на съвместните администратори се разпределят в съответствие с приложение II. Всяка държава членка, която желае да участва в трансграничния обмен на данни между националните мобилни приложения за проследяване на контактите и предупреждаване, преди да се присъедини уведомява Комисията за намерението си и посочва националния или официалния орган, който е бил определен за отговорен администратор.

5. Комисията изпълнява функциите на обработващ личните данни, обработвани в рамките на федерирания портал. В качеството си на обработващ лични данни Комисията гарантира сигурността на обработването, включително предаването и хостването, на лични данни в рамките на федерирания портал и изпълнява установените в приложение III задължения на обработващия лични данни.

6. Ефикасността на техническите и организационните мерки за гарантиране на сигурността на обработването на лични данни в рамките на федерирания портал редовно се подлага на тестване, анализ и оценка от страна на Комисията и на националните органи, оправомощени да имат достъп до федерирания портал.

7. Без да се засяга решението на съвместните администратори за прекратяване на обработването в рамките на федерирания портал, федерираният портал се деактивира не по-късно от 14 дни след като всички свързани национални мобилни приложения за проследяване на контактите и предупреждаване престанат да изпращат ключове посредством федерирания портал.“

6) Приложението става приложение I.

7) Добавят се приложения II и III, чийто текст се съдържа в приложението към настоящото решение.

Член 2

Настоящото решение влиза в сила в деня след деня на публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 15 юли 2020 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ

В Решение за изпълнение 2019/1765 се добавят следните приложения II и III:

„*ПРИЛОЖЕНИЕ II*

ОТГОВОРНОСТИ НА УЧАСТВАЩИТЕ ДЪРЖАВИ ЧЛЕНКИ КАТО СЪВМЕСТНИ АДМИНИСТРАТОРИ НА ФЕДЕРИРАНИЯ ПОРТАЛ ЗА ЦЕЛИТЕ НА ТРАНСГРАНИЧНОТО ОБРАБОТВАНЕ НА ДАННИ МЕЖДУ НАЦИОНАЛНИТЕ МОБИЛНИ ПРИЛОЖЕНИЯ ЗА ПРОСЛЕДЯВАНЕ НА КОНТАКТИТЕ И ПРЕДУПРЕЖДАВАНЕ

РАЗДЕЛ 1

Подраздел 1

Разпределение на отговорностите

1) Съвместните администратори обработват лични данни посредством федерирания портал в съответствие с техническите спецификации, определени от мрежата за електронно здравеопазване ([1]).

2) Всеки администратор отговаря за обработването на лични данни в рамките на федерирания портал в съответствие с Общия регламент относно защитата на данните и Директива 2002/58/ЕО.

3) Всеки администратор създава точка за контакт с функционална пощенска кутия, която ще служи за връзка както между самите съвместни администратори, така и между съвместните администратори и обработващия данните.

4) В съответствие с член 5, параграф 4 мрежата за електронно здравеопазване създава временна подгрупа, натоварена с разглеждането на всякакви въпроси, имащи отношение към оперативната съвместимост на националните мобилни приложения за проследяване на контактите и предупреждаване и от съвместното администриране на свързаното с нея обработване на лични данни, както и към подпомагането координацията на указанията, предавани на Комисията в качеството ѝ на обработващ данните. Наред с други въпроси, в рамките на временната подгрупа администраторите могат да работят по постигането на общ подход по отношение на съхраняването на данни на техните национални бекенд сървъри, като се отчита предвиденият в рамките на федерирания портал период за съхраняване на данни.

5) Указанията за обработващия данните се изпращат от точката за контакт на който и да е от съвместните администратори, съгласувано с останалите съвместни администратори от гореупоменатата подгрупа.

6) Само лица, оправомощени от определените национални или официални органи, могат да имат достъп до личните данни на потребители, обменяни в рамките на федерирания портал.

7) Всеки определен национален орган или официален орган престава да бъде съвместен администратор от датата на оттегляне на участието си във федерирания портал. Той обаче продължава да носи отговорност за обработването на данни в рамките на федерирания портал, извършено преди оттеглянето му.

Подраздел 2

Отговорности и роли във връзка с информирането на субектите на данни и разглеждането на подадени от тях искания

1) В съответствие с членове 13 и 14 от Общия регламент относно защитата на данните всеки администратор предоставя на потребителите на неговите национални мобилни приложения за проследяване на контактите и предупреждаване („субектите на данни“) информация относно обработването на техните лични данни в рамките на федерирания портал за целите на трансграничната оперативна съвместимост на националните мобилни приложения за проследяване на контакти и предупреждаване.

2) Всеки администратор действа като точка за контакт за потребителите на неговото национално мобилно приложение за проследяване на контактите и предупреждаване и разглежда отправени от тези потребители или от техни представители искания, свързани с упражняването на правата на субектите на данни съгласно Общия регламент относно защитата на данните. Всеки администратор определя специална точка за контакт, специализирана в разглеждането на искания, отправени от субектите на данни. Ако съвместен администратор получи искане от субект на данни, което не попада в неговата компетентност, той незабавно го препраща на компетентния съвместен администратор. При поискване съвместните администратори взаимно се подпомагат при разглеждането на искания на субекти на данни и отговарят един на друг без ненужно забавяне, но при всички случаи не по-късно от 15 дни от получаването на искане за помощ.

([1]) Конкретно спецификациите от 16 юни 2020 г. за оперативна съвместимост за трансгранични преносни вериги между одобрени приложения са достъпни на адрес: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0.

3) Всеки администратор довежда до знанието на субектите на данни съдържанието на настоящото приложение, включително разпоредбите по точки 1 и 2.

РАЗДЕЛ 2

Управление на инциденти, свързани със сигурността, включително нарушения на сигурността на личните данни

1) Съвместните администратори взаимно се подпомагат при идентифицирането и реагирането при всякакви инциденти, свързани със сигурността, включително нарушения на сигурността на личните данни, свързани с обработването на данни в рамките на федерирания портал.

2) По-специално съвместните администратори взаимно се уведомяват за:

а) всички потенциални или действителни рискове за наличността, поверителността и/или цялостността на личните данни, които се обработват в рамките на федерирания портал;

б) всякакви инциденти, свързани със сигурността, възникнали във връзка с операцията по обработване в рамките на федерирания портал;

в) всяко нарушение на сигурността на личните данни, вероятните последици от нарушението на сигурността на личните данни и оценката на риска за правата и свободите на физическите лица, както и за всички мерки, предприети за отстраняване на нарушението на сигурността на личните данни и намаляване на риска за правата и свободите на физическите лица;

г) всяко нарушение на техническите и/или организационните гаранции на операцията по обработване в рамките на федерирания портал.

3) В съответствие с членове 33 и 34 от Регламент (ЕС) 2016/679 или след уведомление от Комисията съвместните администратори съобщават на Комисията, на компетентните надзорни органи, а при наличие на такова изискване — и на субектите на данни, за всяко нарушение на сигурността на лични данни, свързано с операцията по обработване в рамките на федерирания портал.

РАЗДЕЛ 3

Оценка на въздействието по отношение на защитата на данните

Ако с оглед на изпълнението на задълженията си, определени в членове 35 и 36 от Общия регламент за защитата на данните, даден администратор се нуждае от информация от друг администратор, той изпраща конкретно искане до функционалната пощенска кутия, посочена в раздел 1, подраздел 1, точка 3). Последният полага всички усилия да предостави информацията.

ПРИЛОЖЕНИЕ III

ОТГОВОРНОСТИ НА КОМИСИЯТА КАТО ОБРАБОТВАЩ ДАННИ В РАМКИТЕ НА ФЕДЕРИРАНИЯ ПОРТАЛ ЗА ЦЕЛИТЕ НА ТРАНСГРАНИЧНОТО ОБРАБОТВАНЕ НА ДАННИ МЕЖДУ НАЦИОНАЛНИТЕ МОБИЛНИ ПРИЛОЖЕНИЯ ЗА ПРОСЛЕДЯВАНЕ НА КОНТАКТИТЕ И ПРЕДУПРЕЖДАВАНЕ

Комисията:

1) Създава и осигурява сигурна и надеждна комуникационна инфраструктура, която осигурява взаимосвързаността на националните мобилни приложения за проследяване на контактите и предупреждаване на държавите членки, участващи във федерирания портал. За целите на изпълнението на нейните задължения като обработващ данни в рамките на федерирания портал, Комисията може да наема трети страни като подизпълнители; Комисията информира съвместните администратори за всяка планирана промяна, свързана с добавяне или замяна на други подизпълнители, като по този начин предоставя на администраторите възможност съвместно да възразят срещу промените, в съответствие с предвиденото в приложение II, раздел 1, подраздел 1, точка 4). Комисията следи за това за тези подизпълнители да важат същите задължения за защита на личните данни като посочените в настоящото решение.

2) Обработва личните данни единствено въз основа на документирани инструкции от администраторите, доколкото не се изисква друго съгласно правото на Съюза или на дадена държава членка; в този случай Комисията информира администраторите за това правно изискване преди обработването, освен когато приложимото законодателство забранява предоставянето на такава информация по важни съображения, свързани с обществения интерес.

3) Обработката от Комисията включва:

а) установяване на автентичността на националните бекенд сървъри въз основа на национални сертификати за бекенд сървъри;

б) приемане на данните по член 7а, параграф 3 от Решението за изпълнение, качвани от националните бекенд сървъри, чрез осигуряване на приложно-програмен интерфейс, позволяващ на националните бекенд сървъри да качват съответните данни;

в) съхраняване на данните във федерирания портал след получаването им от националните бекенд сървъри;

г) предоставяне на данните за изтегляне от националните бекенд сървъри;

д) заличаване на данните след изтеглянето им от всички участващи бекенд сървъри или 14 дни след получаването им, в зависимост от това кое от двете се е случило по-рано;

е) след края на предоставянето на услугата — заличаване на всички останали незаличени данни, освен когато правото на Съюза или на съответната държава членка изисква съхраняването на личните данни.

Обработващият личните данни предприема необходимите мерки за запазване на ненарушимостта на обработваните данни.

4) Предприема всички най-съвременни мерки за осигуряване на организационната, физическата и логическата сигурност с оглед на поддържането на федерирания портал. За тази цел Комисията:

а) определя отговорен субект за управлението на сигурността на равнището на федерирания портал, предава на администраторите информацията за връзка с него и осигурява готовността му да реагира на заплахи за сигурността;

б) носи отговорността за сигурността на федерирания портал;

в) гарантира, че всички физически лица, на които е предоставен достъп до федерирания портал, са обвързани с договорно, професионално или законоустановено задължение за поверителност.

5) Предприема всички необходими мерки за сигурност, така че да не може да се осуети безпрепятственото функциониране на националните бекенд сървъри. За тази цел Комисията въвежда специални процедури отнасящи се до свързването на бекенд сървърите с федерирания портал. Това включва:

а) процедура за оценка на риска, чрез която да се набележат и преценят потенциалните заплахи за системата;

б) процедура за одит и контрол с цел:

i) проверка на съответствието между въведените мерки за сигурност и приложимата политика за сигурност;

ii) редовен контрол на цялостността на системните файлове, на параметрите за сигурност и на дадените разрешения;

iii) мониторинг за откриване на нарушения на сигурността и непозволен достъп;

iv) въвеждане на промени за смекчаване на съществуващи слабости на сигурността;

v) да разрешава, включително по искане на администраторите, и да допринася към извършването на независими одити, включително инспекции, и прегледи на мерките за сигурност, при спазване на условията, свързани с Протокол № 7 към ДФЕС за привилегиите и имунитетите на Европейския съюз ([2]);

([2]) Протокол № 7 за привилегиите и имунитетите на Европейския съюз (ОВ C 326, 26.10.2012 г., стр. 266).

в) промяна на процедурата за контрол с цел документиране и измерване на въздействието на конкретна промяна преди нейното въвеждане и текущо информиране на администраторите за всякакви промени, които могат да засегнат комуникацията с техните инфраструктури и/или сигурността на тези инфраструктури;

г) определяне на процедура за техническа поддръжка и ремонт с цел уточняване на правилата и условията, които да се спазват при необходимост от извършване на техническа поддръжка и ремонт на оборудване;

д) изработване на процедура за инцидентите, свързани със сигурността, с цел определяне на схема за сигнализиране и предаване на сигнала по компетентност, незабавно уведомяване на администраторите и на Европейския надзорен орган по защита на данните за всяко нарушение на сигурността на личните данни и дефиниране на дисциплинарна процедура за разглеждане на нарушения на сигурността.

6) Предприема най-съвременни мерки за осигуряване на физическата и/или логическата сигурност на съоръженията, хостващи оборудването на федерирания портал, както и за проверка на достъпа до логичните данни и сигурността на достъпа. За тази цел Комисията:

а) обезпечава физическата сигурност с цел установяване на отличителни периметри на сигурност и предоставяне на възможност за откриване на нарушения;

б) контролира достъпа до съоръженията и поддържа регистър на посетителите за целите на проследяването;

в) осигурява придружаването на външни хора, получили достъп до помещенията, от служители, които имат необходимото разрешение;

г) гарантира, че не може да бъде добавено, заменено или премахнато оборудване без предварително разрешение на определените отговорни органи;

д) контролира достъпа от националните бекенд сървъри до федерирания портал и от федерирания портал до същите;

е) осигурява идентифициране и удостоверяване на автентичността на физическите лица, които имат достъп до федерирания портал;

ж) преразглежда правата за разрешаване на достъп до федерирания портал в случай на нарушение на сигурността, което засяга тази инфраструктура;

з) пази цялостността на информацията, предадена чрез федерирания портал;

и) въвежда мерки за техническата и организационната сигурност с цел предотвратяване на непозволен достъп до лични данни;

й) въвежда, когато е необходимо, мерки за блокиране на непозволен достъп до федерирания портал от домейна на националните органи (напр. блокиране на местоположение/IP адрес).

7) Предприема стъпки за защита на своя домейн, включително прекъсване на връзките, при значително отклонение от принципите и концепциите за качество или сигурност.

8) Поддържа план за управление на риска в своята област на отговорност.

9) Следи — в реално време — работата на всички компоненти на услугите на федерирания портал, изготвя редовно статистическа информация и води регистри.

10) Предоставя подкрепа за всички услуги на федерирания портал на английски език 24 часа в денонощието, 7 дни седмично, по телефон, по електронна поща или чрез уеб портал и приема обаждания от оправомощени субекти: координаторите на федерирания портал и съответните им бюра за техническо обслужване, администраторите на проекти и определените от Комисията лица.

11) Чрез подходящи технически и организационни мерки доколкото е възможно помага на администраторите да изпълняват задължението си да отговарят на искания във връзка с упражняване на правата на субектите на данни, предвидени в глава III от Общия регламент относно защитата на данните.

12) Оказва подкрепа на администраторите като предоставя информация относно федерирания портал с цел изпълнение на задълженията по членове 32, 35 и 36 от Общия регламент относно защитата на данните.

13) Гарантира, че обработваните в рамките на федерирания портал данни са неразбираеми за лице, което няма разрешение за достъп до тях.

14) Предприема всички подходящи мерки за предотвратяване на непозволен достъп на операторите на федерирания портал до предаваните данни.

15) Предприема мерки за по-висока степен на оперативна съвместимост и за по-добра комуникация между определените администратори на федерирания портал.

16) Поддържа регистър на дейностите по обработване, извършвани от името на администраторите в съответствие с член 31, параграф 2 от Регламент (ЕС) 2018/1725.“