II

(Nem jogalkotási aktusok)

HATÁROZATOK

A BIZOTTSÁG (EU) 2020/1023 VÉGREHAJTÁSI HATÁROZATA

(2020. július 15.)

az (EU) 2019/1765 végrehajtási határozatnak a COVID19-világjárvány elleni küzdelem céljából a kontaktkövető és figyelmeztető mobilalkalmazások közötti, határokon átnyúló adatcsere tekintetében történő módosításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről szóló, 2011. március 9-i 2011/24/EU európai parlamenti és tanácsi irányelvre ([1]) és különösen annak 14. cikke (3) bekezdésére,

mivel:

(1) A 2011/24/EU irányelv 14. cikke azt a feladatot rótta az Európai Unióra, hogy támogassa és segítse elő a tagállamok által kijelölt, az e-egészségügyért felelős nemzeti hatóságokat összekötő önkéntes hálózat (a továbbiakban: e-egészségügyi hálózat) keretében tevékenykedő tagállamok közötti együttműködést és információcserét.

(2) Az (EU) 2019/1765 bizottsági végrehajtási határozat ([2]) meghatározza az e-egészségügyért felelős nemzeti hatóságok hálózatának létrehozására, igazgatására és működésére vonatkozó szabályokat. Az említett határozat 4. cikke azzal a feladattal bízza meg az e-egészségügyi hálózatot, hogy segítse elő a nemzeti információs és kommunikációs technológiai rendszerek nagyobb fokú interoperabilitását, valamint az elektronikus egészségügyi adatoknak a határon átnyúló egészségügyi ellátás keretében való átadhatóságát.

(3) A COVID19-világjárvány által okozott népegészségügyi válsághelyzetben több tagállam olyan mobilalkalmazásokat fejlesztett ki, amelyek támogatják a kontaktkövetést, és lehetővé teszik ezen alkalmazások felhasználói számára, hogy amennyiben potenciálisan ki voltak téve a vírusnak egy olyan másik felhasználó közelsége miatt, aki az alkalmazás révén bejelentette, hogy vírustesztje pozitív lett, riasztást kapjanak és megtegyék a megfelelő intézkedést (például tesztelés vagy otthoni karantén). Ezek az alkalmazások Bluetooth-technológiát használnak, hogy észleljék, amikor az eszközök egymás közelébe kerülnek. Mivel 2020 júniusa óta megszűntek a tagállamok közötti utazásra vonatkozó korlátozások, az e-egészségügyi hálózat keretében a tagállamok között nagyobb interoperabilitást kell elérni a nemzeti információs és kommunikációs technológiai rendszerek között, olyan digitális infrastruktúra létrehozásával, amely lehetővé teszi a kontaktkövetést és a figyelmeztetést támogató nemzeti mobilalkalmazások közötti interoperabilitást.

([1]) HL L 88., 2011.4.4., 45. o.

([2]) A Bizottság (EU) 2019/1765 végrehajtási határozata (2019. október 22.) az e-egészségügyért felelős nemzeti hatóságok hálózatának létrehozására, igazgatására és működésére vonatkozó szabályok meghatározásáról és a 2011/890/EU végrehajtási határozat hatályon kívül helyezéséről (HL L 270., 2019.10.24., 83. o.).

(4) A Bizottság támogatja a tagállamokat a fent említett mobilalkalmazások tekintetében. A Bizottság 2020. április 8-án ajánlást fogadott el a COVID19-válság leküzdéséhez és az abból való kilábaláshoz szükséges technológia és adatok használatára szolgáló közös uniós eszköztárról, különösen a mobilalkalmazások és az anonimizált mobilitási adatok tekintetében (a továbbiakban: az ajánlás) ([3]). Az e-egészségügyi hálózatban részt vevő tagállamok a Bizottság támogatásával a tagállamoknak szóló közös uniós eszköztárat fogadtak el a kontaktkövető mobilalkalmazásokra vonatkozóan ([4]), valamint interoperabilitási iránymutatásokat fogadtak el a jóváhagyott kontaktkövető mobilalkalmazások Európai Unióban történő használatát illetően ([5]). Az eszköztár ismerteti a nemzeti kontaktkövető és figyelmeztető alkalmazásokra vonatkozó nemzeti követelményeket, különösen arra vonatkozóan, hogy az alkalmazások használatának önkéntes alapon kell történnie, az alkalmazásokat az adott nemzeti egészségügyi hatóságnak jóvá kell hagynia, azoknak tiszteletben kell tartaniuk a magánéletet, valamint hogy amint már nincs szükség rájuk, azokat el kell távolítani. A COVID19-válsággal összefüggő legújabb fejleményeket követően a Bizottság ([6]) és az Európai Adatvédelmi Testület ([7]) egy-egy iránymutatást adott ki az adatvédelemmel összefüggésben a mobilalkalmazásokról és a kontaktkövető eszközökről. A tagállamok mobilalkalmazásainak és az interoperabilitást lehetővé tevő digitális infrastruktúrájuknak a kialakítása a közös uniós eszköztárra, a fent említett iránymutatásra és az e-egészségügyi hálózatban elfogadott műszaki előírásokra épül.

(5) A nemzeti kontaktkövető és figyelmeztető mobilalkalmazások interoperabilitásának elősegítése érdekében az e-egészségügyi hálózatban részt vevő azon tagállamok, amelyek önkéntes alapon fokozni kívánják együttműködésüket ezen a területen, a Bizottság támogatásával digitális infrastruktúrát alakítottak ki az adatcsere informatikai biztosítására. Erre a digitális infrastruktúrára a továbbiakban „egyesítőportálként" történik hivatkozás.

(6) Ez a határozat megállapítja a részt vevő tagállamoknak és a Bizottságnak a nemzeti kontaktkövető és figyelmeztető mobilalkalmazások határokon átnyúló interoperabilitását szolgáló egyesítőportál működtetésében betöltött szerepére vonatkozó rendelkezéseket.

(7) A kontaktkövető és figyelmeztető mobilalkalmazások felhasználói személyes adatainak kezelését, amelyért a tagállamok vagy más tagállami közintézmények vagy szervek felelősek, az (EU) 2016/679 európai parlamenti és tanácsi rendelettel ([8]) (a továbbiakban: általános adatvédelmi rendelet) és a 2002/58/EK európai parlamenti és tanácsi irányelvvel ([9]) összhangban kell végezni. A személyes adatoknak a Bizottság általi, az egyesítőportál biztonságának irányítása és megvalósítása céljából történő kezelése az (EU) 2018/1725 európai parlamenti és tanácsi rendeletnek ([10]) megfelelően kell, hogy történjen.

(8) Az egyesítőportálnak egy közös interfészt biztosító biztonságos informatikai infrastruktúrából kell állnia, amelyen belül a kijelölt nemzeti hatóságok vagy hivatalos szervek megoszthatják egymással a SARS-CoV-2 vírussal fertőzött személyekkel való kapcsolattartásra vonatkozó minimális adatokat annak érdekében, hogy tájékoztathassanak másokat az e fertőzésnek való lehetséges kitettségükről, és a releváns információk megosztásával előmozdítsák a tagállamok közötti hatékony együttműködést az egészségügyi ellátás terén.

(9) E határozatnak ezért meg kell határoznia a kijelölt nemzeti hatóságok vagy hivatalos szervek között az egyesítőportálon keresztül az EU-n belül folytatott, határokon átnyúló adatcsere szabályait.

([3]) A Bizottság (EU) 2020/518 ajánlása (2020. április 8.) a COVID-19-válság leküzdéséhez és az abból való kilábaláshoz szükséges technológia és adatok, különösen a mobilalkalmazások és az anonimizált mobilitási adatok használatára szolgáló közös uniós eszköztárról (HL L 114., 2020.4.14., 7. o.).

([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]) A Bizottság közleménye – Iránymutatás az adatvédelemmel összefüggésben a COVID19-világjárvány elleni küzdelmet támogató alkalmazásokról (HL C 124I., 2020.4.17., 1. o.).

([7]) 04/2020 sz. iránymutatás a COVID19-járvánnyal összefüggésben a helymeghatározó adatok és a kontaktkövető eszközök használatáról, valamint az Európai Adatvédelmi Testület 2020. június 16-i nyilatkozata a kontaktkövető alkalmazások interoperabilitásának adatvédelmi hatásairól, mindkettő megtekinthető a következő weboldalon: https://edpb.europa.eu

([8]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

([9]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o.).

([10]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

(10) A részt vevő tagállamok, amelyeket a kijelölt nemzeti hatóságok vagy hivatalos szervek képviselnek, közösen határozzák meg a személyes adatok egyesítőportálon keresztül történő feldolgozásának célját és eszközeit, ezért ezen adatok közös adatkezelőinek tekintendők. Az általános adatvédelmi rendelet 26. cikke kötelezettségként előírja, hogy a személyes adatok kezelésével kapcsolatos műveleteket végző közös adatkezelőknek átlátható módon kell meghatározniuk a rendeletekben foglalt kötelezettségek teljesítésével kapcsolatos felelősségi körök megoszlását. Rendelkezik továbbá arról a lehetőségről is, hogy e felelősségi köröket az adatkezelőkre alkalmazandó uniós vagy tagállami jog határozza meg. Minden adatkezelőnek meg kell győződnie arról, hogy nemzeti szinten jogalappal rendelkezik az egyesítőportálon történő adatfeldolgozás tekintetében.

(11) A Bizottság az egyesítőportál technikai és szervezési megoldásait biztosító intézményként a részt vevő tagállamok nevében közös adatkezelőként álnevesített személyes adatokat kezel az egyesítőportálon, ezért adatfeldolgozónak tekintendő. Az általános adatvédelmi rendelet 28. cikke és az (EU) 2018/1725 rendelet 29. cikke értelmében az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben, és amely meghatározza az adatkezelést. Ez a határozat a Bizottság által adatfeldolgozóként végzett adatkezelésre vonatkozó szabályokat határozza meg.

(12) A személyes adatoknak az egyesítőportál keretében történő kezelése során a Bizottságra nézve kötelező erővel bír az (EU, Euratom) 2017/46 bizottsági határozat ([11]).

(13) mivel azok a célok, amelyek érdekében az adatkezelők a nemzeti kontaktkövető és figyelmeztető mobilalkalmazásokkal továbbított személyes adatokat dolgoznak fel, nem feltétlenül igénylik az érintettek azonosítását, az adatkezelők nem mindig vannak abban a helyzetben, hogy biztosítsák az érintettek jogainak alkalmazását. Az általános adatvédelmi rendelet 15–20. cikkében említett jogok ezért adott esetben nem alkalmazhatók, ha az említett rendelet 11. cikke szerinti feltételek teljesülnek.

(14) Az (EU) 2019/1765 végrehajtási határozat meglévő mellékletét két új melléklet beillesztése miatt újra kell számozni.

(15) Az (EU) 2019/1765 végrehajtási határozatot ezért ennek megfelelően módosítani kell.

(16) Tekintettel a COVID19-világjárvány által kiváltott helyzet sürgősségére, ezt a határozatot az Európai Unió Hivatalos Lapjában való kihirdetését követő naptól kell alkalmazni.

(17) Az (EU) 2018/1725 rendelet 42. cikkének (1) bekezdésével összhangban konzultációra került sor az európai adatvédelmi biztossal, aki 2020. július 9-én nyilvánított véleményt.

(18) Az e határozatban előírt intézkedések összhangban vannak a 2011/24/EU irányelv 16. cikke alapján létrehozott bizottság véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Az (EU) 2019/1765 végrehajtási határozat a következőképpen módosul:

1. A 2. cikk (1) bekezdése a következő g), h), i), j), k), l), m), n) és o) ponttal egészül ki:

„g) »alkalmazás felhasználója«: intelligens eszközzel rendelkező személy, aki jóváhagyott kontaktkövető és figyelmeztető mobilalkalmazást töltött le és futtat;

h) »kontaktkövetés«: a határokon átterjedő súlyos egészségügyi veszélynek kitett személyek nyomon követése céljából végrehajtott intézkedések az 1082/2013/EU európai parlamenti és tanácsi határozat (*) 3. cikkének c) pontja értelmében;

([11]) A Bizottság (EU, Euratom) 2017/46 határozata (2017. január 10.) az Európai Bizottság kommunikációs és információs rendszereinek biztonságáról (HL L 6., 2017.1.11., 40. o.). A Bizottság további információt tesz közzé az Európai Bizottság informatikai rendszereire vonatkozó biztonsági előírásokkal kapcsolatban az alábbi weboldalon: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en.

i) »nemzeti kontaktkövető és figyelmeztető mobilalkalmazás«: olyan, nemzeti szinten jóváhagyott, intelligens eszközökön, különösen okostelefonokon futó szoftveralkalmazás, amelyet általában webes forrásokkal való széles körű és célzott interakcióra terveztek, és amely az intelligens eszközökben megtalálható különféle érzékelők által gyűjtött, közelségre vonatkozó adatokat és egyéb háttér-információkat dolgoz fel a SARS-CoV-2 által fertőzött személyekkel való érintkezés nyomon követése és a SARS-CoV-2 vírusnak esetlegesen kitett személyek figyelmeztetése céljából. Ezek a mobilalkalmazások képesek kimutatni a Bluetooth-technológiát használó más eszközök jelenlétét, és az internet segítségével képesek információt cserélni backend szerverekkel;

j) »egyesítőportál«: a Bizottság által egy biztonságos informatikai eszközön keresztül működtetett hálózati felület, amely a nemzeti kontaktkövető és figyelmeztető mobilalkalmazások interoperabilitásának biztosítása céljából a személyes adatok minimális körét fogadja, tárolja és teszi elérhetővé a tagállamok backend szerverei között;

k) »kulcs«: az alkalmazás egy olyan felhasználójához kapcsolódó egyedi ideiglenes azonosító, aki jelenti, hogy megfertőződött a SARS-CoV-2 vírussal, illetve hogy SARS-CoV-2 vírussal fertőzött személlyel érintkezhetett;

l) »fertőzöttség ellenőrzése«: a SARS-CoV-2-fertőzés megerősítésére alkalmazott módszer annak megállapítására, hogy a fertőzöttséget az alkalmazás felhasználója saját maga jelentette-e be, vagy a fertőzöttség megállapítása nemzeti egészségügyi hatóság megerősítésének vagy laboratóriumi vizsgálatnak az eredménye-e;

m) »érintett országok«: az az egy vagy több tagállam, amelyben az alkalmazás felhasználója a kulcsok feltöltését megelőző 14 napos időszakban tartózkodott és letöltötte a jóváhagyott nemzeti kontaktkövető és figyelmeztető alkalmazást, és/vagy ahová az említett időszakban utazott;

n) »a kulcsok származási országa«: azon tagállam, amelyben a kulcsokat a közös portálra feltöltő backend szerver található;

o) »naplóadat«: az egyesítőportálon keresztül feldolgozott adatok cseréjével és az azokhoz való hozzáféréssel kapcsolatos tevékenység automatikus nyilvántartása, amely feltünteti különösen az adatkezelési tevékenység típusát, az adatkezelési tevékenység napját és időpontját, valamint az adatkezelést végző személy azonosítóját.

_____

(*) (*) Az Európai Parlament és a Tanács 1082/2013/EU határozata (2013. október 22.) a határokon átterjedő súlyos egészségügyi veszélyekről és a 2119/98/EK határozat hatályon kívül helyezéséről (HL L 293., 2013.11.5., 1. o.).”

2. A 4. cikk (1) bekezdése a következő h) ponttal egészül ki:

„h) iránymutatást nyújt a tagállamoknak a személyes adatok nemzeti kontaktkövető és figyelmeztető mobilalkalmazások közötti, egyesítőportálon keresztül történő, határokon átnyúló cseréjéről.”

3. A 6. cikk (1) bekezdése a következő f) és g) ponttal egészül ki:

„f) az egyesítőportálon található személyes adatok továbbításának és tárolásának biztonságával kapcsolatban megfelelő technikai és szervezési intézkedéseket dolgoz ki, hajt végre és tart fenn a nemzeti kontaktkövető és figyelmeztető mobilalkalmazások interoperabilitásának biztosítására;

g) a szükséges vizsgálatok és ellenőrzések biztosítása és végrehajtása révén támogatást nyújt az e-egészségügyi hálózatnak az arról való egyetértés kidolgozásában, hogy a nemzeti hatóságok megfelelnek-e az egyesítőportálon található személyes adatok határokon átnyúló cseréjére vonatkozó technikai és szervezési követelményeknek. A Bizottság szakértőinek munkáját tagállami szakértők segíthetik.”

4. A 7. cikk a következőképpen módosul:

a) a cím helyébe „Az e-egészségügyi digitális szolgáltatási infrastruktúrán keresztül feldolgozott személyes adatok védelme” lép;

b) a (2) bekezdésben a „mellékletében” szöveg helyébe az „I. mellékletében” szöveg lép.

5. A rendelet a következő 7a. cikkel egészül ki:

„*7a. cikk*

A személyes adatok nemzeti kontaktkövető és figyelmeztető mobilalkalmazások közötti, egyesítőportálon keresztül történő, határokon átnyúló cseréje

(1) Az egyesítőportálon keresztül megosztott személyes adatok esetében az adatkezelés kizárólag a nemzeti kontaktkövető és figyelmeztető mobilalkalmazások interoperabilitásának megkönnyítését és a kontaktkövetés határokon átnyúló összefüggésben biztosítandó folyamatosságát szolgálhatja.

(2) A (3) bekezdésben említett személyes adatok álnevesített formátumban kerülnek továbbításra az egyesítőportálra.

(3) Az egyesítőportálon keresztül megosztott és abban feldolgozott, álnevesített személyes adatok kizárólag a következő információkat tartalmazhatják:

a) a nemzeti kontaktkövető és figyelmeztető mobilalkalmazások által a kulcsok feltöltése előtt legfeljebb 14 nappal továbbított kulcsok;

b) a kulcsokhoz kapcsolódó naplóadatok a kulcsok származási országában használt műszaki előírásokban található protokollnak megfelelően;

c) a fertőzöttség ellenőrzése;

d) az érintett országok és a kulcsok származási országa.

(4) Az egyesítőportálon található személyes adatokat kezelő kijelölt nemzeti hatóságok vagy hivatalos szervek az egyesítőportálon feldolgozott adatok közös adatkezelői. A közös adatkezelők felelősségi köreit a II. mellékletnek megfelelően kell kiosztani. A személyes adatok nemzeti kontaktkövető és figyelmeztető mobilalkalmazások közötti határokon átnyúló cseréjében részt venni kívánó tagállamok szándékukról a csatlakozásuk előtt értesítik a Bizottságot, feltüntetve a közös adatkezelőként kijelölt nemzeti hatóságot vagy hivatalos szervet.

(5) A Bizottság az egyesítőportálon belül feldolgozott személyes adatok feldolgozója. Adatfeldolgozóként a Bizottság gondoskodik az adatkezelés biztonságáról, többek között az egyesítőportálon található személyes adatok továbbításának és tárolásának biztonságáról, és teljesíti a III. mellékletben meghatározott adatfeldolgozói kötelezettségeit.

(6) A Bizottság és az egyesítőportálhoz való hozzáférésre jogosult nemzeti hatóságok rendszeresen tesztelik, elemzik és értékelik a személyes adatok egyesítőportálon belüli kezelésének biztonságát garantáló technikai és szervezési intézkedések hatékonyságát.

(7) A közös adatkezelőknek az egyesítőportálon való adatkezelés befejezésére vonatkozó határozatának sérelme nélkül az egyesítőportál működését legkésőbb 14 nappal azt követően meg kell szüntetni, hogy az összes kapcsolódó nemzeti kontaktkövető és figyelmeztető mobilalkalmazás beszünteti az egyesítőportálon keresztül történő kulcstovábbítást.”

6. A melléklet I. mellékletre módosul.

7. A határozat egy II. és egy III. melléklettel egészül ki, amelyek szövegét ennek a határozatnak a melléklete tartalmazza.

2. cikk

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon lép hatályba.

Kelt Brüsszelben, 2020. július 15-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

MELLÉKLET

Az (EU) 2019/1765 végrehajtási határozat a következő II. és III. melléklettel egészül ki:

'II. MELLÉKLET

A RÉSZT VEVŐ TAGÁLLAMOKNAK MINT A NEMZETI KONTAKTKÖVETŐ ÉS FIGYELMEZTETŐ MOBILALKALMAZÁSOK KÖZÖTTI, HATÁROKON ÁTNYÚLÓ ADATKEZELÉST SZOLGÁLÓ EGYESÍTŐPORTÁL KÖZÖS ADATKEZELŐINEK A FELELŐSSÉGI KÖRE

1. SZAKASZ

1. alszakasz

A felelősségi körök megosztása

1. A közös adatkezelők az e-egészségügyi hálózat keretében elfogadott műszaki előírásoknak megfelelően ([1]) kezelik az egyesítőportálon továbbított személyes adatokat.

2. Minden adatkezelő felelős azért, hogy a személyes adatoknak az egyesítőportálon történő kezelése az általános adatvédelmi rendelettel és a 2002/58/EK irányelvvel összhangban történjen.

3. Minden adatkezelő létrehoz egy kapcsolattartó pontot, és azt egy funkcionális postafiókkal látja el a közös adatkezelők közötti, valamint a közös adatkezelők és az adatfeldolgozó közötti kommunikáció biztosítására.

4. Az e-egészségügyi hálózat által az 5. cikk (4) bekezdésével összhangban létrehozott ideiglenes alcsoport feladata, hogy megvizsgálja a nemzeti kontaktkövető és figyelmeztető mobilalkalmazások interoperabilitásával, valamint a kapcsolódó személyes adatok kezelésére irányuló közös adatkezeléssel kapcsolatos problémákat, és segítse a Bizottságnak mint adatfeldolgozónak szóló összehangolt utasítások kidolgozását. Az adatkezelők az ideiglenes alcsoport keretében többek között közös megközelítést dolgozhatnak ki az adatoknak a nemzeti backend szervereiken való megőrzésére vonatkozóan, figyelembe véve az egyesítőportálon meghatározott megőrzési időszakot.

5. Az adatfeldolgozónak szóló utasításokat a közös adatkezelők valamely kapcsolattartó pontja küldi meg, a fent említett alcsoportban tevékeny többi közös adatkezelő hozzájárulásával.

6. Az egyesítőportálon keresztül megosztott felhasználói személyes adatokhoz kizárólag a kijelölt nemzeti hatóságok vagy hivatalos szervek által felhatalmazott személyek férhetnek hozzá.

7. Az egyes kijelölt nemzeti hatóságok vagy hivatalos szervek közös adatkezelői minősége az egyesítőportálon való részvételük visszavonásának időpontjában megszűnik. Az említett hatóságok vagy szervek azonban továbbra is felelősek az egyesítőportálon a részvételük megszűnését megelőzően folytatott adatkezelésért.

2. alszakasz

Az érintettek kéréseinek kezelésével és az érintettek tájékoztatásával kapcsolatos felelősségi körök és feladatok

1. Az egyes adatkezelők – az általános adatvédelmi rendelet 13. és 14. cikkével összhangban – tájékoztatják nemzeti kontaktkövető és figyelmeztető mobilalkalmazásuk felhasználóit (a továbbiakban: az érintettek) személyes adataiknak az egyesítőportálon a nemzeti kontaktkövető és figyelmeztető mobilalkalmazások interoperabilitásának biztosítása céljából történő kezeléséről.

2. Az egyes adatkezelők kapcsolattartó pontként szolgálnak a nemzeti kontaktkövető és figyelmeztető mobilalkalmazásuk felhasználói számára, és foglalkoznak az érintettek jogainak az általános adatvédelmi rendelettel összhangban történő gyakorlásával kapcsolatos, az említett felhasználók vagy képviselőik által benyújtott kérelmekkel. Minden adatkezelő külön kapcsolattartó pontot jelöl ki az érintettek kérelmeinek feldolgozása céljából. Amennyiben egy közös adatkezelőhöz valamely érintettől olyan kérelem érkezik, amely nem tartozik a felelősségi körébe, akkor azt haladéktalanul továbbítja az azért felelős közös adatkezelőnek. A közös adatkezelők kérésre segítik egymást az érintettek kérelmeinek kezelésében, és indokolatlan késedelem nélkül, de legkésőbb a segítségnyújtás iránti kérelem kézhezvételétől számított 15 napon belül választ adnak egymásnak.

([1]) Különösen a jóváhagyott alkalmazásokra vonatkozó, a több tagállamot érintő fertőzési láncok esetében alkalmazandó 2020. június 16-i interoperabilitási előírásoknak megfelelően, amelyek az alábbi címen érhetők el: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

3. Az egyes adatkezelők az érintettek rendelkezésére bocsátják e melléklet tartalmát, beleértve az 1. és 2. pontban megállapított szabályokat is.

2. SZAKASZ

A biztonsági események – többek között az adatvédelmi incidensek – kezelése

1. A közös adatkezelők segítik egymást a biztonsági események azonosításában és kezelésében, ideértve az adatvédelmi incidensek azon eseteit is, amelyek az egyesítőportálon történő adatkezeléshez kapcsolódnak.

2. A közös adatkezelők különösen a következőkről értesítik egymást:

a) az egyesítőportálon kezelt személyes adatok rendelkezésre állását, bizalmas jellegét és/vagy sértetlenségét érintő esetleges vagy tényleges kockázatok;

b) az egyesítőportálon végzett adatkezelési műveletekhez kapcsolódó biztonsági események;

c) adatvédelmi incidensek, az adatvédelmi incidens valószínűsíthető következményei, a természetes személyek jogait és szabadságait érintő kockázatok értékelése, valamint az adatvédelmi incidens kezelése és a természetes személyek jogait és szabadságait érintő kockázatok csökkentése érdekében hozott intézkedések;

d) az egyesítőportálon végzett adatkezelési műveletek technikai és/vagy szervezési biztosítékainak megsértése.

3. A közös adatkezelők az (EU) 2016/679 rendelet 3és 34. cikkével összhangban vagy a Bizottság által küldött értesítést követően tájékoztatják a Bizottságot, az illetékes felügyeleti hatóságokat és szükség esetén az érintetteket az egyesítőportálon végzett adatkezelési műveletekkel kapcsolatos minden adatvédelmi incidensről.

3. SZAKASZ

Adatvédelmi hatásvizsgálat

Ha egy adatkezelőnek az általános adatvédelmi rendelet 35. és 36. cikkében meghatározott kötelezettségei teljesítése érdekében egy másik adatkezelőtől információra van szüksége, erre irányulóan kérelmet kell küldenie az 1. szakasz 1. alszakaszának 3. pontjában említett funkcionális postafiókba. A másik adatkezelő minden tőle telhetőt megtesz a szóban forgó információk rendelkezésre bocsátása érdekében.

III. MELLÉKLET

A BIZOTTSÁGNAK MINT A NEMZETI KONTAKTKÖVETŐ ÉS FIGYELMEZTETŐ MOBILALKALMAZÁSOK KÖZÖTTI, HATÁROKON ÁTNYÚLÓ ADATKEZELÉST SZOLGÁLÓ EGYESÍTŐPORTÁL ADATFELDOLGOZÓJÁNAK A FELELŐSSÉGI KÖRE

A Bizottság feladatai:

1. A Bizottság egy olyan biztonságos és megbízható kommunikációs infrastruktúrát hoz létre és bocsát rendelkezésre, amely összekapcsolja az egyesítőportálon részt vevő tagállamok nemzeti kontaktkövető és figyelmeztető mobilalkalmazásait. Az egyesítőportál adatfeldolgozójaként rá háruló kötelezettségek teljesítése érdekében a Bizottság harmadik feleket is megbízhat további adatfeldolgozóként; a Bizottság tájékoztatja a közös adatkezelőket az egyéb további adatfeldolgozók megbízásával vagy leváltásával kapcsolatos tervezett változtatásokról, ezáltal lehetővé téve az adatkezelők számára, hogy a II. melléklet 1. szakasza 1. alszakasza 4. pontjának megfelelően közösen kifogást emeljenek az ilyen változtatások ellen. A Bizottság gondoskodik arról, hogy az e határozatban foglalt adatvédelmi kötelezettségek az említett további adatfeldolgozókra is alkalmazandók legyenek.

2. A Bizottság a személyes adatokat kizárólag az adatkezelők dokumentált utasításai alapján kezeli, kivéve, ha az adatok kezelésére uniós vagy tagállami jogszabály vonatkozik; ebben az esetben a Bizottság az adatfeldolgozást megelőzően tájékoztatja az adatkezelőket az említett jogi előírásról, kivéve, ha a szóban forgó jogszabály fontos közérdekből tiltja az ilyen tájékoztatást.

3. A Bizottság által végzett adatkezelés a következőket foglalja magában:

a) a nemzeti backend szerverek nemzeti backendszerver-tanúsítványok alapján történő hitelesítése;

b) a végrehajtási határozat 7a. cikkének (3) bekezdésében említett, a nemzeti backend szerverek által feltöltött adatok fogadása egy olyan alkalmazásprogramozási felületen, amely lehetővé teszi a nemzeti backend szerverek számára a megfelelő adatok feltöltését;

c) az adatoknak a nemzeti backend szerverekről való beérkezését követően azok tárolása az egyesítőportálon;

d) az adatok rendelkezésre bocsátása a nemzeti backend szerverek általi letöltés céljából;

e) az adatok törlése azoknak az összes részt vevő backend szerver általi letöltése után, illetve a beérkezésüket követő 14 nap elteltével, attól függően, hogy melyik a korábbi időpont;

f) minden fennmaradó adat törlése a szolgáltatásnyújtás végét követően, kivéve, ha uniós vagy tagállami jogszabály előírja a személyes adatok tárolását.

Az adatfeldolgozó megteszi a szükséges intézkedéseket a kezelt adatok sértetlenségének biztosítására.

4. Az egyesítőportál karbantartása érdekében a Bizottság meghoz minden korszerű szervezeti, fizikai és logikai jellegű biztonsági intézkedést. A Bizottság e célból:

a) kijelöl egy, az egyesítőportál biztonsági irányításáért felelős szervezetet, közli az adatkezelőkkel annak elérhetőségét, és biztosítja, hogy az képes legyen reagálni a biztonsági fenyegetésekre;

b) felelősséget vállal az egyesítőportál biztonságáért;

c) biztosítja, hogy az egyesítőportálhoz hozzáféréssel rendelkező valamennyi személyre szerződéses, szakmai vagy jogszabályban előírt titoktartási kötelezettség vonatkozzon;

5. A Bizottság minden szükséges biztonsági intézkedést megtesz annak érdekében, hogy a nemzeti backend szerverek zavartalan működése ne kerüljön veszélybe. E célból a Bizottság megalkotja a backend szervereknek az egyesítőportálra történő csatlakozásával kapcsolatos konkrét eljárásokat. Ezek az alábbiakat foglalják magukban:

a) kockázatértékelési eljárás a rendszert fenyegető potenciális veszélyek azonosítása és mértékük megbecslése érdekében;

b) ellenőrzési és felülvizsgálati eljárás a következők céljából:

   i. a végrehajtott biztonsági intézkedések és az alkalmazandó biztonsági politika közötti megfelelés ellenőrzése;

   ii. a rendszerfájlok, a biztonsági paraméterek és a megadott engedélyek megbízhatóságának rendszeres ellenőrzése;

   iii. a biztonság megsértésének és a behatolásoknak az észlelése érdekében történő nyomon követés;

   iv. módosítások végrehajtása a meglévő biztonsági hiányosságok csökkentése érdekében; valamint

   v. a független ellenőrzések elvégzésének lehetővé tétele, többek között az adatkezelők kérésére, és az azokhoz történő hozzájárulás, ideértve a biztonsági intézkedésekkel kapcsolatos ellenőrzéseket és felülvizsgálatokat is, az EUMSZ-hez csatolt, az Európai Unió kiváltságairól és mentességeiről szóló 7. jegyzőkönyvet ([2]) tiszteletben tartó feltételek mellett;

([2]) Az Európai Unió kiváltságairól és mentességeiről szóló 7. jegyzőkönyv (HL C 326., 2012.10.26., 266. o.).

c) az ellenőrzési eljárás módosítása annak érdekében, hogy a módosítás végrehajtása előtt dokumentálható és értékelhető legyen a változás hatása, és hogy az adatkezelők tájékoztatást kapjanak minden olyan változásról, amely hatással lehet az infrastruktúráikkal való kommunikációra és/vagy azok biztonságára;

d) karbantartási és javítási eljárások meghatározása a berendezések karbantartása és/vagy javítása esetén követendő szabályok és feltételek meghatározása céljából;

e) biztonsági incidensekre vonatkozó eljárás meghatározása a jelentési és eszkalációs rendszer meghatározására, az adatkezelők és az európai adatvédelmi biztos késedelem nélküli tájékoztatására minden adatvédelmi incidensről, valamint a biztonság megsértése esetén fegyelmi eljárás meghatározása.

6. A Bizottság a technika állásának megfelelő fizikai és/vagy logikai biztonsági intézkedéseket hoz az egyesítőportál berendezéseinek otthont adó létesítmények számára, valamint a logikai adatok és a biztonsági hozzáférés ellenőrzése tekintetében. A Bizottság e célból:

a) érvényre juttatja a fizikai biztonságot a különleges biztonsági övezetek kialakítása és a jogsértések felderítése érdekében;

b) ellenőrzi a létesítményekhez való hozzáférést, és nyomon követés céljából nyilvántartást vezet a látogatókról;

c) biztosítja, hogy az épületekbe való belépési engedéllyel rendelkező külső személyeket megfelelő felhatalmazással rendelkező személyzet kísérje;

d) biztosítja, hogy a kijelölt felelős szervek előzetes engedélye nélkül ne kerülhessen sor berendezések bevitelére, cseréjére vagy eltávolítására;

e) ellenőrzi a nemzeti backend szerverek és az egyesítőportál egymáshoz való hozzáférését;

f) biztosítja az egyesítőportálhoz való hozzáféréssel rendelkező személyek azonosítását és hitelesítését;

g) felülvizsgálja az egyesítőportálhoz való hozzáféréssel kapcsolatos engedélyezési jogokat abban az esetben, ha az infrastruktúra biztonsága sérül;

h) megőrzi az egyesítőportálon keresztül továbbított információk sértetlenségét;

i) technikai és szervezési biztonsági intézkedéseket vezet be a személyes adatokhoz való jogosulatlan hozzáférés megakadályozására;

j) szükség esetén olyan intézkedéseket hajt végre, amelyek lehetővé teszik az egyesítőportálhoz való, a nemzeti hatóságok domainjéről kiinduló jogosulatlan hozzáférések megakadályozását (pl. helyszín/IP-cím blokkolása).

7. A minőség és a biztonság alapelveitől és fogalmaitól való lényeges eltérés esetén a Bizottság lépéseket tesz a domain védelme érdekében, ideértve a kapcsolatok megszakítását is.

8. A felelősségi körével kapcsolatban kockázatkezelési tervet tart fenn.

9. Figyelemmel kíséri – valós időben – az egyesítőportál valamennyi szolgáltatási elemének teljesítményét, rendszeres statisztikákat készít és nyilvántartást vezet.

10. Napi 24 órában telefonon, e-mailben vagy egy webportálon keresztül angol nyelven támogatást nyújt az egyesítőportál valamennyi szolgáltatásához, és fogadja az engedélyezett hívó felek – az egyesítőportál koordinátorai és azok ügyfélszolgálatai, a projektfelelősök és a Bizottság által kijelölt személyek – hívásait.

11. A Bizottság – a lehetőségek függvényében – megfelelő technikai és szervezési intézkedésekkel támogatást nyújt az adatkezelőknek azon kötelezettségük teljesítéséhez, hogy válaszoljanak az érintettek jogainak gyakorlásával kapcsolatos kérelmekre, mely jogokat az általános adatvédelmi rendelet III. fejezete határozza meg.

12. Az általános adatvédelmi rendelet 32., 35. és 36. cikke szerinti kötelezettségek teljesítése érdekében a Bizottság az egyesítőportálra vonatkozó információk megadásával támogatja az adatkezelőket.

13. A Bizottság gondoskodik arról, hogy az egyesítőportálon kezelt adatok minden, hozzáférési jogosultsággal nem rendelkező személy számára értelmezhetetlenek legyenek.

14. A Bizottság minden szükséges intézkedést megtesz annak megakadályozására, hogy az egyesítőportál működtetői jogosulatlanul hozzáférhessenek a továbbított adatokhoz.

15. A Bizottság intézkedéseket hoz, hogy elősegítse az egyesítőportál kijelölt adatkezelői közötti interoperabilitást és kommunikációt.

16. A Bizottság az (EU) 2018/1725 rendelet 31. cikke (2) bekezdésének megfelelően nyilvántartást vezet az adatkezelők nevében végzett adatkezelési tevékenységekről.’