II

(Akty o charakterze nieustawodawczym)

DECYZJE

DECYZJA WYKONAWCZA KOMISJI (UE) 2020/1023

z dnia 15 lipca 2020 r.

zmieniająca decyzję wykonawczą (UE) 2019/1765 w zakresie transgranicznej wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania w związku ze zwalczaniem pandemii COVID-19

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej ([1]), w szczególności jej art. 14 ust. 3,

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 14 dyrektywy 2011/24/UE do zadań Unii należy wspieranie i ułatwianie współpracy oraz wymiany informacji między państwami członkowskimi działającymi w ramach dobrowolnej sieci skupiającej wyznaczone przez państwa członkowskie organy krajowe odpowiedzialne za e-zdrowie („sieć e-zdrowie").

(2) W decyzji wykonawczej Komisji (UE) 2019/1765 ([2]) ustanowiono zasady niezbędne do utworzenia sieci e-zdrowie skupiającej organy krajowe odpowiedzialne za e-zdrowie, zarządzania tą siecią i jej funkcjonowania. W art. 4 tej decyzji sieci e-zdrowie powierzono zadanie ułatwiania większej interoperacyjności krajowych systemów ICT oraz transgranicznej przenoszalności elektronicznych danych dotyczących zdrowia w transgranicznej opiece zdrowotnej.

(3) W świetle kryzysu w dziedzinie zdrowia publicznego spowodowanego pandemią COVID-19 kilka państw członkowskich opracowało aplikacje mobilne wspomagające ustalanie kontaktów zakaźnych i umożliwiające użytkownikom takich aplikacji otrzymywanie powiadomień o konieczności podjęcia odpowiednich działań, takich jak zgłoszenie się na badanie lub samoizolacja, jeżeli mogli mieć styczność z wirusem w związku z bliskim kontaktem z innym użytkownikiem takiej aplikacji, u którego zdiagnozowano zakażenie wirusem. Aplikacje te działają w oparciu o technologię Bluetooth i wykrywają inne urządzenia znajdujące się w pobliżu. W miarę znoszenia – począwszy od czerwca 2020 r. – ograniczeń podróży między państwami członkowskimi należy zapewnić większą interoperacyjność krajowych systemów ICT między państwami członkowskimi w ramach sieci e-zdrowie poprzez wdrażanie cyfrowej infrastruktury umożliwiającej interoperacyjność między krajowymi aplikacjami mobilnymi wspomagającymi ustalanie kontaktów zakaźnych i ostrzeganie.

([1]) Dz.U. L 88 z 4.4.2011, s. 45.

([2]) Decyzja wykonawcza Komisji (UE) 2019/1765 z dnia 22 października 2019 r. ustanawiająca zasady utworzenia sieci organów krajowych odpowiedzialnych za e-zdrowie, zarządzania tą siecią i jej funkcjonowania oraz uchylająca decyzję wykonawczą 2011/890/UE (Dz.U. L 270 z 24.10.2019, s. 83).

(4) Komisja wspiera państwa członkowskie w zakresie wspomnianych aplikacji mobilnych. W dniu 8 kwietnia 2020 r. Komisja przyjęła zalecenie w sprawie wspólnego unijnego zestawu instrumentów ułatwiającego wykorzystanie technologii i danych w celu zwalczania kryzysu wywołanego przez COVID-19 i wyjścia z niego, w szczególności w odniesieniu do aplikacji mobilnych i wykorzystywania zanonimizowanych danych dotyczących mobilności („zalecenie Komisji") ([3]). Przy wsparciu ze strony Komisji państwa członkowskie w ramach sieci e-zdrowie przyjęły – z myślą o państwach członkowskich – wspólny unijny zestaw instrumentów na potrzeby aplikacji mobilnych mający na celu wspieranie ustalania kontaktów zakaźnych ([4]) oraz wytyczne dotyczące interoperacyjności zatwierdzonych aplikacji mobilnych służących do ustalania kontaktów zakaźnych w UE ([5]). Zestaw instrumentów obejmuje wyjaśnienie krajowych wymogów dotyczących krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania – w szczególności wskazanie, że powinny one być dobrowolne, zatwierdzone przez właściwy krajowy organ ds. zdrowia, powinny chronić prywatność oraz zostać zdezaktywowane, gdy nie będą już dłużej potrzebne. W świetle rozwoju sytuacji związanej z kryzysem spowodowanym przez COVID-19 Komisja ([6]) oraz Europejska Rada Ochrony Danych ([7]) wydały wytyczne dotyczące aplikacji mobilnych i narzędzi do ustalania kontaktów zakaźnych w kontekście ochrony danych osobowych. Tworzenie aplikacji mobilnych państw członkowskich i budowa infrastruktury cyfrowej umożliwiającej ich interoperacyjność przebiegają w oparciu o wspólny unijny zestaw instrumentów, wspomniane powyżej wytyczne oraz specyfikacje techniczne uzgodnione w ramach sieci e-zdrowie.

(5) Aby umożliwić interoperacyjność krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania, przy wsparciu ze strony Komisji państwa członkowskie uczestniczące w sieci e-zdrowie, które dobrowolnie zdecydowały się na zacieśnianie współpracy w tym obszarze, opracowały infrastrukturę cyfrową jako narzędzie IT służące do wymiany danych. Wspomniana infrastruktura cyfrowa jest dalej zwana „bramą federacyjną" (ang. *federation gateway*).

(6) W niniejszej decyzji ustanowiono przepisy regulujące rolę uczestniczących państw członkowskich oraz Komisji w funkcjonowaniu bramy federacyjnej wykorzystywanej do zapewnienia transgranicznej interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania.

(7) Przetwarzanie danych osobowych użytkowników aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania, za który to proces odpowiadają państwa członkowskie lub inne organizacje publiczne bądź organy urzędowe w państwach członkowskich, należy prowadzić zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 ([8]) („ogólne rozporządzenie o ochronie danych") oraz dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady ([9]). Przetwarzanie danych osobowych, za które odpowiada Komisja, w celu zarządzania bramą federacyjną oraz zapewnienia jej bezpieczeństwa powinno przebiegać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725 ([10]).

(8) Brama federacyjna powinna obejmować bezpieczną infrastrukturę IT zapewniającą wspólny interfejs, za pośrednictwem którego wyznaczone organy krajowe lub organy urzędowe mogą wymieniać między sobą minimalne zbiory danych na temat kontaktów użytkowników aplikacji z osobami zakażonymi SARS-CoV-2 w celu informowania tych użytkowników o potencjalnym narażeniu na zakażenie i w celu promowania skutecznej współpracy w zakresie opieki zdrowotnej między państwami członkowskimi poprzez ułatwianie wymiany odpowiednich informacji.

(9) W niniejszej decyzji należy zatem określić tryb transgranicznej wymiany danych między wyznaczonymi organami krajowymi lub organami urzędowymi w UE za pośrednictwem bramy federacyjnej.

([3]) Zalecenie Komisji (UE) 2020/518 z dnia 8 kwietnia 2020 r. w sprawie wspólnego unijnego zestawu instrumentów ułatwiającego wykorzystanie technologii i danych w celu zwalczania kryzysu wywołanego przez COVID-19 i wyjścia z niego, w szczególności w odniesieniu do aplikacji mobilnych i wykorzystywania zanonimizowanych danych dotyczących mobilności (Dz.U. L 114 z 14.4.2020, s. 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]) Komunikat Komisji: Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych (Dz. U. C 124I z 17.4.2020, s. 1).

([7]) Wytyczne 04/2020 w sprawie wykorzystywania danych dotyczących lokalizacji oraz narzędzi służących do ustalania kontaktów zakaźnych w kontekście pandemii COVID-19 oraz Oświadczenie EROD w sprawie interoperacyjności aplikacji służących do ustalania kontaktów zakaźnych z dnia 16 czerwca 2020 r.; oba dokumenty są dostępne pod adresem: https://edpb.europa.eu/edpb_pl.

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

([9]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

(10) Uczestniczące państwa członkowskie, reprezentowane przez wyznaczone organy krajowe lub organy urzędowe, wspólnie wyznaczają cel i określają sposoby przetwarzania danych osobowych za pośrednictwem bramy federacyjnej, a zatem są współadministratorami. W art. 26 ogólnego rozporządzenia o ochronie danych na współadministratorów prowadzących operacje przetwarzania danych osobowych nałożono wymóg określenia w przejrzysty sposób odpowiednich zakresów ich odpowiedzialności za wypełnianie obowiązków wynikających z tego rozporządzenia. W artykule tym przewidziano również, że spoczywające na współadministratorach obowiązki i ich zakres mogą być określone przez prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. Każdy z administratorów powinien zapewnić, aby na szczeblu krajowym dysponował podstawą prawną przetwarzania za pośrednictwem bramy federacyjnej.

(11) Komisja, zapewniając rozwiązania techniczne i organizacyjne na potrzeby bramy federacyjnej, przetwarza za jej pośrednictwem pseudonimiczne dane osobowe w imieniu uczestniczących państw członkowskich jako współadministratorów, a zatem jest ona podmiotem przetwarzającym. Zgodnie z art. 28 ogólnego rozporządzenia o ochronie danych i art. 29 rozporządzenia (UE) 2018/1725 przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora oraz określają przetwarzanie danych. W niniejszej decyzji ustanowiono zasady przetwarzania danych przez Komisję w roli podmiotu przetwarzającego.

(12) Podczas przetwarzania danych osobowych w ramach bramy federacyjnej Komisję obowiązuje decyzja Komisji (UE, Euratom) 2017/46 ([11]).

(13) Biorąc pod uwagę fakt, że cele, dla których administratorzy przetwarzają dane osobowe w krajowych aplikacjach mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania, niekoniecznie wymagają identyfikacji osoby, której dane dotyczą, administratorzy mogą nie zawsze być w stanie zapewnić, by osoba, której dane dotyczą, mogła korzystać z przysługujących jej praw. Prawa, o których mowa w art. 15–20 ogólnego rozporządzenia o ochronie danych, mogą zatem nie mieć zastosowania, gdy spełnione są warunki określone w art. 11 tego rozporządzenia.

(14) Należy zmienić numer obecnego załącznika do decyzji wykonawczej (UE) 2019/1765, ponieważ dodano dwa nowe załączniki.

(15) Należy zatem odpowiednio zmienić decyzję wykonawczą (UE) 2019/1765.

(16) Ze względu na pilny charakter sytuacji spowodowanej pandemią COVID-19 niniejsza decyzja powinna mieć zastosowanie od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

(17) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 9 lipca 2020 r.

(18) Środki przewidziane w niniejszej decyzji są zgodne z opinią Komitetu ustanowionego na mocy art. 16 dyrektywy 2011/24/UE,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

W decyzji wykonawczej (UE) 2019/1765 wprowadza się następujące zmiany:

1) w art. 2 ust. 1 dodaje się litery g), h), i), j), k), l), m), n) i o) w brzmieniu:

„g) »użytkownik aplikacji« oznacza osobę posiadającą urządzenie inteligentne, która pobrała i uruchomiła zatwierdzoną aplikację mobilną służącą do ustalania kontaktów zakaźnych i ostrzegania;

h) »ustalanie kontaktów zakaźnych« oznacza środki stosowane w celu wykrycia osób, które były narażone na działanie źródła poważnego transgranicznego zagrożenia zdrowia, w rozumieniu art. 3 lit. c) decyzji Parlamentu Europejskiego i Rady nr 1082/2013/UE (*);

([11]) Decyzja Komisji (UE, Euratom) 2017/46 z dnia 10 stycznia 2017 r. w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej (Dz.U. L 6 z 11.1.2017, s. 40). Komisja publikuje dalsze informacje na temat norm bezpieczeństwa mających zastosowanie do wszystkich systemów informatycznych Komisji Europejskiej pod adresem: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_pl.

i) »krajowa aplikacja mobilna służąca do ustalania kontaktów zakaźnych i ostrzegania« oznacza zatwierdzone na szczeblu krajowym oprogramowanie działające na urządzeniach inteligentnych, w szczególności smartfonach, zaprojektowane zazwyczaj do szeroko zakrojonej i ukierunkowanej interakcji z zasobami internetowymi, które przetwarza dane dotyczące bliskości fizycznej i inne informacje kontekstowe gromadzone za pomocą wielu czujników, w które wyposażone są urządzenia inteligentne, w celu wykrywania kontaktów z osobami zakażonymi SARS-CoV-2 i ostrzegania osób, które mogły mieć styczność z SARS-CoV-2. Wspomniane aplikacje mobilne mają możliwość wykrywania obecności innych urządzeń korzystających z technologii Bluetooth i wymiany informacji z serwerami wewnętrznymi (ang. *backend servers*) przy użyciu internetu;

j) »brama federacyjna« oznacza bramę sieciową obsługiwaną przez Komisję za pomocą bezpiecznego narzędzia IT, która służy do odbierania, przechowywania i udostępniania minimalnego zbioru danych osobowych między serwerami wewnętrznymi państw członkowskich w celu zapewnienia interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania;

k) »klucz« oznacza niepowtarzalny efemeryczny identyfikator przypisany użytkownikowi aplikacji, który zgłasza, że został zakażony SARS-CoV-2, lub który mógł mieć styczność z SARS-CoV-2;

l) »weryfikacja zakażenia« oznacza metodę stosowaną w celu potwierdzenia zakażenia SARS-CoV-2, tj. zgłoszenie zakażenia przez użytkownika aplikacji, potwierdzenie zakażenia przez krajowy organ ds. zdrowia lub zakażenie potwierdzone badaniem laboratoryjnym;

m) »państwa będące przedmiotem zainteresowania« oznaczają państwo członkowskie lub państwa członkowskie, w których użytkownik aplikacji przebywał w okresie 14 dni poprzedzających datę przesłania kluczy i w których pobrał zatwierdzoną krajową aplikację mobilną służącą do ustalania kontaktów zakaźnych i ostrzegania lub do których podróżował;

n) »państwo pochodzenia kluczy« oznacza państwo członkowskie, w którym zlokalizowany jest serwer wewnętrzny, który przesłał klucze do bramy federacyjnej;

o) »dane dziennika« oznaczają automatyczny zapis czynności związanej z wymianą danych przetworzonych za pośrednictwem bramy federacyjnej oraz uzyskaniem dostępu do nich, który w szczególności obejmuje rodzaj czynności przetwarzania, datę i czas tej czynności oraz identyfikator osoby przetwarzającej dane.

_____

(*) Decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE (Dz.U. L 293 z 5.11.2013, s. 1).";

2) w art. 4 ust. 1 dodaje się literę h) w brzmieniu:

„h) zapewnić państwom członkowskim wytyczne dotyczące transgranicznej wymiany danych osobowych za pośrednictwem bramy federacyjnej między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania.";

3) w art. 6 ust. 1 dodaje się lit. f) i g) w brzmieniu:

„f) opracowuje, wdraża i obsługuje odpowiednie środki techniczne i organizacyjne związane z bezpieczeństwem przesyłu i przechowywania danych osobowych w bramie federacyjnej na potrzeby zapewnienia interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania;

g) wspiera sieć e-zdrowie w procesie stwierdzania technicznej i organizacyjnej zgodności organów krajowych z wymogami dotyczącymi transgranicznej wymiany danych osobowych za pośrednictwem bramy federacyjnej, zapewniając i przeprowadzając niezbędne badania i audyty. Audytorów Komisji mogą wspierać eksperci z państw członkowskich.";

4) w art. 7 wprowadza się następujące zmiany:

a) tytuł otrzymuje brzmienie „Ochrona danych osobowych przetwarzanych za pośrednictwem europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia";

b) w ust. 2 słowo „załączniku" zastępuje się słowami „załączniku I";

5) dodaje się art. 7a w brzmieniu:

„*Artykuł 7a*

Transgraniczna wymiana danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania za pośrednictwem bramy federacyjnej

1. Jeżeli dane osobowe są wymieniane za pośrednictwem bramy federacyjnej, przetwarzanie ogranicza się do celów dotyczących ułatwienia interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania w ramach bramy federacyjnej oraz zapewnienia ciągłości procesu ustalania kontaktów zakaźnych w kontekście transgranicznym.

2. Dane osobowe, o których mowa w ust. 3, są przekazywane do bramy federacyjnej w formacie pseudonimicznym.

3. Pseudonimiczne dane osobowe wymieniane oraz przetwarzane za pośrednictwem bramy federacyjnej obejmują jedynie następujące informacje:

a) klucze przekazane przez krajowe aplikacje mobilne służące do ustalania kontaktów zakaźnych i ostrzegania w okresie do 14 dni poprzedzających datę przesłania kluczy;

b) dane dziennika dotyczące kluczy zgodnie z protokołem specyfikacji technicznych stosowanym w państwie pochodzenia kluczy;

c) weryfikację zakażenia;

d) państwa będące przedmiotem zainteresowania oraz państwo pochodzenia kluczy.

4. Wyznaczone organy krajowe lub organy urzędowe przetwarzające dane osobowe za pośrednictwem bramy federacyjnej są współadministratorami danych przetwarzanych za pośrednictwem bramy federacyjnej. Podział odpowiednich obowiązków między współadministratorami przebiega zgodnie z załącznikiem II. Każde państwo członkowskie, które chce uczestniczyć w transgranicznej wymianie danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania, przed przystąpieniem zawiadamia Komisję o swoim zamiarze i wskazuje organ krajowy lub organ urzędowy wyznaczony jako odpowiedzialny administrator.

5. Komisja jest podmiotem przetwarzającym dane osobowe, które podlegają przetwarzaniu za pośrednictwem bramy federacyjnej. Do kompetencji Komisji jako podmiotu przetwarzającego należy zapewnienie bezpieczeństwa przetwarzania – w tym przesyłu i przechowywania – danych osobowych w ramach bramy federacyjnej oraz wypełnianie obowiązków podmiotu przetwarzającego określonych w załączniku III.

6. Skuteczność środków technicznych i organizacyjnych mających na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych za pośrednictwem bramy federacyjnej jest regularnie sprawdzana i oceniana przez Komisję oraz przez organy krajowe upoważnione do dostępu do bramy federacyjnej.

7. Bez uszczerbku dla decyzji współadministratorów o zakończeniu przetwarzania za pośrednictwem bramy federacyjnej brama federacyjna ulega dezaktywacji najpóźniej 14 dni po zakończeniu przekazywania kluczy za jej pośrednictwem przez wszystkie połączone krajowe aplikacje mobilne służące do ustalania kontaktów zakaźnych i ostrzegania.";

6) załącznik staje się załącznikiem I;

7) dodaje się załączniki II i III w brzmieniu określonym w załączniku do niniejszej decyzji.

Artykuł 2

Niniejsza decyzja wchodzi w życie następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 15 lipca 2020 r.

W imieniu Komisji
Ursula VON DER LEYEN
Przewodnicząca

ZAŁĄCZNIK

W decyzji wykonawczej (UE) 2019/1765 dodaje się załączniki II i III w brzmieniu:

„ZAŁĄCZNIK II

OBOWIĄZKI UCZESTNICZĄCYCH PAŃSTW CZŁONKOWSKICH JAKO WSPÓŁADMINISTRATORÓW NA POTRZEBY BRAMY FEDERACYJNEJ DO CELÓW TRANSGRANICZNEGO PRZETWARZANIA MIĘDZY KRAJOWYMI APLIKACJAMI MOBILNYMI SŁUŻĄCYMI DO USTALANIA KONTAKTÓW ZAKAŹNYCH I OSTRZEGANIA

SEKCJA 1

Podsekcja 1

Podział obowiązków

1. Współadministratorzy przetwarzają dane osobowe za pośrednictwem bramy federacyjnej zgodnie ze specyfikacjami technicznymi określonymi przez sieć e-zdrowie ([1]).

2. Każdy administrator odpowiada za przetwarzanie danych osobowych za pośrednictwem bramy federacyjnej zgodnie z ogólnym rozporządzeniem o ochronie danych i dyrektywą 2002/58/WE.

3. Każdy administrator ustanawia punkt kontaktowy posiadający funkcyjną skrzynkę pocztową, która będzie służyć do komunikacji między współadministratorami oraz między współadministratorami a podmiotem przetwarzającym.

4. Tymczasowa podgrupa utworzona przez sieć e-zdrowie zgodnie z art. 5 ust. 4 ma za zadanie analizowanie wszelkich kwestii wynikających z interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania oraz ze współadministrowania powiązanym przetwarzaniem danych osobowych, a także ułatwianie wydawania skoordynowanych instrukcji dla Komisji jako podmiotu przetwarzającego. W ramach tymczasowej podgrupy administratorzy mogą prowadzić prace mające na celu m.in. wypracowanie wspólnego podejścia do przechowywania danych na ich krajowych serwerach wewnętrznych, z uwzględnieniem okresu przechowywania danych określonego w ramach bramy federacyjnej.

5. Instrukcje dla podmiotu przetwarzającego są wysyłane przez punkt kontaktowy któregokolwiek z współadministratorów w porozumieniu z pozostałymi współadministratorami wchodzącymi w skład wspomnianej powyżej podgrupy.

6. Wyłącznie osoby uprawnione przez wyznaczone organy krajowe lub organy urzędowe mogą mieć dostęp do danych osobowych użytkowników, które to dane są przekazywane za pośrednictwem bramy federacyjnej.

7. Każdy wyznaczony organ krajowy lub organ urzędowy przestaje być współadministratorem od dnia wycofania swojego udziału w bramie federacyjnej. Pozostaje on jednak odpowiedzialny za przetwarzanie za pośrednictwem bramy federacyjnej, które miało miejsce przed jego wycofaniem się.

Podsekcja 2

Obowiązki i role w zakresie rozpatrywania wniosków osób, których dane dotyczą, oraz w zakresie informowania takich osób

1. Każdy administrator przekazuje użytkownikom swojej krajowej aplikacji mobilnej służącej do ustalania kontaktów zakaźnych i ostrzegania (»osoby, których dane dotyczą«) informacje na temat przetwarzania ich danych osobowych za pośrednictwem bramy federacyjnej do celów transgranicznej interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania zgodnie z art. 13 i 14 ogólnego rozporządzenia o ochronie danych.

2. Każdy administrator pełni rolę punktu kontaktowego dla użytkowników jego krajowej aplikacji mobilnej służącej do ustalania kontaktów zakaźnych i ostrzegania oraz rozpatruje składane przez tych użytkowników lub ich przedstawicieli wnioski związane z wykonywaniem praw osób, których dane dotyczą, zgodnie z ogólnym rozporządzeniem o ochronie danych. Każdy administrator wyznacza specjalny punkt kontaktowy zajmujący się rozpatrywaniem wniosków otrzymanych od osób, których dane dotyczą. Jeżeli współadministrator otrzyma od osoby, której dane dotyczą, wniosek, który nie wchodzi w zakres jego odpowiedzialności, niezwłocznie przekazuje go odpowiedzialnemu współadministratorowi. Jeżeli zostaną o to poproszeni, współadministratorzy pomagają sobie nawzajem w rozpatrywaniu wniosków osób, których dane dotyczą, i udzielają sobie nawzajem odpowiedzi bez zbędnej zwłoki, przy czym nie później niż w terminie 15 dni od otrzymania prośby o udzielenie pomocy.

([1]) W szczególności specyfikacje dotyczące interoperacyjności dla transgranicznych łańcuchów transmisji między zatwierdzonymi aplikacjami z dnia 16 czerwca 2020 r. dostępne pod adresem: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0.

3. Każdy administrator udostępnia osobom, których dane dotyczą, treść niniejszego załącznika, w tym ustalenia określone w pkt 1 i 2.

SEKCJA 2

Zarządzanie cyberincydentami, w tym naruszeniami ochrony danych osobowych

1. Współadministratorzy pomagają sobie nawzajem w identyfikacji cyberincydentów i reagowaniu na cyberincydenty, w tym w przypadku naruszeń ochrony danych osobowych, w związku z przetwarzaniem za pośrednictwem bramy federacyjnej.

2. Współadministratorzy w szczególności powiadamiają się nawzajem o kwestiach takich, jak:

a) wszelkie potencjalne lub faktyczne ryzyko dla dostępności, poufności lub integralności danych osobowych przetwarzanych za pośrednictwem bramy federacyjnej;

b) wszelkie cyberincydenty związane z operacją przetwarzania za pośrednictwem bramy federacyjnej;

c) każde naruszenie ochrony danych osobowych, prawdopodobne konsekwencje naruszenia ochrony danych osobowych oraz ocena ryzyka naruszenia praw i wolności osób fizycznych, a także wszelkie środki wdrożone w celu przeciwdziałania naruszaniu ochrony danych osobowych i łagodzenia ryzyka naruszenia praw i wolności osób fizycznych;

d) każde naruszenie technicznych lub organizacyjnych zabezpieczeń dotyczących operacji przetwarzania za pośrednictwem bramy federacyjnej.

3. Współadministratorzy powiadamiają o wszelkich naruszeniach ochrony danych osobowych odnoszących się do operacji przetwarzania za pośrednictwem bramy federacyjnej Komisję, właściwe organy nadzorcze i, jeśli jest to wymagane, osoby, których dane dotyczą, zgodnie z art. 33 i 34 rozporządzenia (UE) 2016/679 lub po otrzymaniu powiadomienia ze strony Komisji.

SEKCJA 3

Ocena skutków dla ochrony danych

Jeżeli w celu wypełnienia obowiązków określonych w art. 35 i 36 ogólnego rozporządzenia o ochronie danych administrator potrzebuje informacji od innego administratora, wysyła specjalny wniosek na adres funkcjonalnej skrzynki pocztowej, o której mowa w sekcji 1 podsekcja 1 pkt 3. Administrator, który otrzymał taki wniosek, dokłada wszelkich starań, aby takie informacje przekazać.

ZAŁĄCZNIK III

OBOWIĄZKI KOMISJI JAKO PODMIOTU PRZETWARZAJĄCEGO DANE NA POTRZEBY BRAMY FEDERACYJNEJ DO CELÓW TRANSGRANICZNEGO PRZETWARZANIA MIĘDZY KRAJOWYMI APLIKACJAMI MOBILNYMI SŁUŻĄCYMI DO USTALANIA KONTAKTÓW ZAKAŹNYCH I OSTRZEGANIA

Komisja:

1. Tworzy i zapewnia bezpieczną i niezawodną infrastrukturę łączności, która łączy krajowe aplikacje mobilne służące do ustalania kontaktów zakaźnych i ostrzegania państw członkowskich uczestniczących w bramie federacyjnej. Aby wywiązać się ze swoich obowiązków jako podmiotu przetwarzającego dane w ramach bramy federacyjnej, Komisja może zaangażować osoby trzecie jako podwykonawców podmiotu przetwarzającego dane; Komisja informuje współadministratorów o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podwykonawców podmiotu przetwarzającego dane, dając tym samym administratorom możliwość wspólnego wyrażenia sprzeciwu wobec takich zmian, jak określono w załączniku II sekcja 1 podsekcja 1 pkt 4. Komisja zapewnia, aby do tych podwykonawców podmiotu przetwarzającego dane zastosowanie miały takie same obowiązki dotyczące ochrony danych osobowych jak te określone w niniejszej decyzji.
2. Przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratorów, chyba że obowiązek taki nakłada na nią prawo Unii lub prawo państwa członkowskiego; w takim przypadku przed rozpoczęciem przetwarzania Komisja informuje administratorów o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
3. Przetwarzanie danych przez Komisję obejmuje:

a) uwierzytelnianie krajowych serwerów wewnętrznych (ang. *back-end servers*) na podstawie krajowych certyfikatów serwerów wewnętrznych;

b) odbiór danych, o których mowa w art. 7a ust. 3 decyzji wykonawczej, przesłanych przez krajowe serwery wewnętrzne poprzez zapewnienie interfejsu programowania aplikacji, który umożliwia krajowym serwerom wewnętrznym przesyłanie odpowiednich danych;

c) przechowywanie danych w bramie federacyjnej po otrzymaniu ich z krajowych serwerów wewnętrznych;

d) udostępnianie danych do pobrania przez krajowe serwery wewnętrzne;

e) usuwanie danych po ich pobraniu przez wszystkie uczestniczące serwery wewnętrzne lub po upływie 14 dni od ich odbioru w zależności od tego, co nastąpi wcześniej;

f) po zakończeniu świadczenia usługi usuwa wszelkie pozostałe dane, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

Podmiot przetwarzający wprowadza niezbędne środki w celu zachowania integralności przetwarzanych danych.

4. Wprowadza wszelkie najnowocześniejsze organizacyjne, fizyczne i logiczne środki bezpieczeństwa służące utrzymaniu bramy federacyjnej. W tym celu Komisja:

a) wyznacza podmiot odpowiedzialny za zarządzanie bezpieczeństwem na poziomie bramy federacyjnej, przekazuje administratorom dane kontaktowe tego podmiotu oraz zapewnia jego dostępność w celu reagowania na zagrożenia dla bezpieczeństwa;

b) przyjmuje odpowiedzialność za bezpieczeństwo bramy federacyjnej;

c) zapewnia, aby wszystkie osoby, którym przyznano dostęp do bramy federacyjnej, podlegały umownemu, zawodowemu lub ustawowemu obowiązkowi zachowania poufności.

5. Wprowadza wszelkie niezbędne środki bezpieczeństwa, aby nie dopuścić do zakłócenia sprawnego funkcjonowania operacyjnego krajowych serwerów wewnętrznych. W tym celu Komisja wprowadza szczególne procedury związane z połączeniem serwerów wewnętrznych z bramą federacyjną. Obejmuje to:

a) procedurę oceny ryzyka, by wykryć i oszacować potencjalne zagrożenia dla systemu;

b) procedurę audytu i przeglądu, aby:

   (i) sprawdzać, czy wprowadzane środki bezpieczeństwa odpowiadają postanowieniom mającej zastosowanie polityki bezpieczeństwa;

   (ii) przeprowadzać regularne kontrole integralności plików systemowych, parametrów bezpieczeństwa i przyznanych zezwoleń;

   (iii) prowadzić monitorowanie w celu wykrywania naruszeń bezpieczeństwa i włamań;

   (iv) wdrażać zmiany, których celem jest ograniczenie istniejących uchybień w zakresie bezpieczeństwa;

   (v) umożliwić, w tym na wniosek administratorów, przeprowadzanie niezależnych audytów, w tym kontroli, oraz przeglądów środków bezpieczeństwa, oraz wnosić wkład w przeprowadzanie tych audytów, kontroli i przeglądów, z zastrzeżeniem warunków, które są zgodne z Protokołem (nr 7) do TFUE w sprawie przywilejów i immunitetów Unii Europejskiej ([2]);

([2]) Protokół (nr 7) w sprawie przywilejów i immunitetów Unii Europejskiej (Dz.U. C 326 z 26.10.2012, s. 266).

c) zmianę procedury kontroli, by udokumentować i zmierzyć wpływ zmiany przed jej wdrożeniem oraz na bieżąco informować administratorów o wszelkich zmianach, które mogą wpłynąć na łączność z ich infrastrukturą lub na bezpieczeństwo ich infrastruktury;

d) określenie procedury konserwacji i naprawy, by określić zasady i warunki, których należy przestrzegać w przypadku konieczności przeprowadzenia konserwacji lub naprawy sprzętu;

e) ustanowienie procedury dotyczącej cyberincydentu, by określić system zgłaszania i eskalacji, bezzwłocznie informować administratorów oraz Europejskiego Inspektora Ochrony Danych o wszelkich naruszeniach ochrony danych osobowych, a także określić procedurę dyscyplinarną w przypadku naruszeń bezpieczeństwa.

6. Wprowadza najnowocześniejsze fizyczne lub logiczne środki bezpieczeństwa w odniesieniu do obiektów, w których znajduje się sprzęt bramy federacyjnej, oraz w odniesieniu do kontroli dostępu do danych logicznych i kontroli bezpiecznego dostępu. W tym celu Komisja:

a) egzekwuje bezpieczeństwo fizyczne, by ustanowić wyraźne granice bezpieczeństwa i umożliwić wykrywanie naruszeń;

b) kontroluje dostęp do obiektów i prowadzi rejestr odwiedzających do celów identyfikacyjnych;

c) zapewnia, aby osobom z zewnątrz, którym udzielono dostępu do obiektów, towarzyszył odpowiednio upoważniony członek personelu;

d) zapewnia, aby sprzętu nie można było dodać, wymienić ani usunąć bez uprzedniej zgody wyznaczonych odpowiedzialnych podmiotów;

e) kontroluje dostęp z oraz do krajowych serwerów wewnętrznych do bramy federacyjnej;

f) zapewnia, aby osoby, które uzyskują dostęp do bramy federacyjnej, zostały zidentyfikowane i uwierzytelnione;

g) dokonuje przeglądu uprawnień do udzielania zezwoleń na dostęp do bramy federacyjnej w przypadku wykrycia naruszenia bezpieczeństwa mającego wpływ na tę infrastrukturę;

h) zachowuje integralność informacji przekazywanych za pośrednictwem bramy federacyjnej;

i) wprowadza techniczne i organizacyjne środki bezpieczeństwa, by zapobiec nieuprawnionemu dostępowi do danych osobowych;

j) wprowadza – w razie potrzeby – środki mające na celu zablokowanie nieuprawnionego dostępu do bramy federacyjnej z domeny organów krajowych (tj. zablokowanie lokalizacji/adresu IP).

7. Podejmuje kroki w celu ochrony swojej domeny, obejmujące zerwanie połączeń, w przypadku znacznych odstępstw od zasad i koncepcji jakości lub bezpieczeństwa.

8. Utrzymuje plan zarządzania ryzykiem związany ze swoim zakresem odpowiedzialności.

9. Monitoruje – w czasie rzeczywistym – wydajność wszystkich komponentów usług w ramach bramy federacyjnej, tworzy regularne statystyki i prowadzi rejestry.

10. Zapewnia wsparcie w odniesieniu do wszystkich usług w ramach bramy federacyjnej – w języku angielskim, całodobowo, przez siedem dni w tygodniu, drogą telefoniczną, mailową lub za pośrednictwem portalu internetowego – oraz odbiera połączenia od upoważnionych osób dzwoniących: koordynatorów bramy federacyjnej oraz pracowników ich odpowiednich działów pomocy technicznej, specjalistów ds. projektów i wyznaczonych osób z Komisji.

11. W miarę możliwości wspiera administratorów za pośrednictwem odpowiednich środków technicznych i organizacyjnych w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III ogólnego rozporządzenia o ochronie danych.

12. Wspiera administratorów poprzez przekazywanie im informacji na temat bramy federacyjnej w celu realizacji obowiązków przewidzianych w art. 32, 35 i 36 ogólnego rozporządzenia o ochronie danych.

13. Zapewnia, aby dane przetwarzane w ramach bramy federacyjnej były niemożliwe do odczytania dla każdej osoby, która nie jest uprawniona do uzyskania do nich dostępu.

14. Wprowadza wszelkie odpowiednie środki, by zapobiec sytuacji, w której operatorzy bramy federacyjnej mogliby uzyskać nieuprawniony dostęp do przekazywanych danych.

15. Wprowadza środki mające na celu ułatwienie interoperacyjności i łączności między wyznaczonymi administratorami bramy federacyjnej.

16. Prowadzi rejestr czynności przetwarzania dokonywanych w imieniu administratorów zgodnie z art. 31 ust. 2 rozporządzenia (UE) 2018/1725.”.