►B

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

(notyfikowana jako dokument nr C(2019) 7460)

(Tekst mający znaczenie dla EOG)

(Dz.U. L 270 z 24.10.2019, s. 83)

zmieniona przez:

		Dziennik Urzędowy		
		nr	strona	data
►M1	Decyzja wykonawcza Komisji (UE) 2020/1023 z dnia 15 lipca 2020 r.	L 227 I	1	16.7.2020

▼B

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

(notyfikowana jako dokument nr C(2019) 7460)

(Tekst mający znaczenie dla EOG)

Artykuł 1

Przedmiot

W niniejszej decyzji ustanawia się zasady niezbędne do utworzenia sieci e-zdrowie skupiającej organy krajowe odpowiedzialne za e-zdrowie, zarządzania tą siecią i jej funkcjonowania, zgodnie z art. 14 dyrektywy 2011/24/UE.

Artykuł 2

Definicje

1. Do celów niniejszej decyzji:

a) „sieć e-zdrowie” oznacza dobrowolną sieć skupiającą wyznaczone przez państwa członkowskie organy krajowe odpowiedzialne za e-zdrowie i realizującą cele określone w art. 14 dyrektywy 2011/24/UE;

b) „krajowe punkty kontaktowe ds. e-zdrowia” oznaczają organizacyjne i techniczne bramki umożliwiające świadczenie transgranicznych usług informacyjnych w dziedzinie e-zdrowia, za które odpowiadają państwa członkowskie;

c) „transgraniczne usługi informacyjne w dziedzinie e-zdrowia” oznaczają istniejące usługi przetwarzane za pośrednictwem krajowych punktów kontaktowych ds. e-zdrowia i poprzez platformę usług podstawowych opracowaną przez Komisję w celu świadczenia transgranicznej opieki zdrowotnej;

d) „europejska infrastruktura usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia” oznacza infrastrukturę, która umożliwia świadczenie transgranicznych usług informacyjnych w dziedzinie e-zdrowia za pośrednictwem krajowych punktów kontaktowych ds. e-zdrowia oraz europejskiej platformy usług podstawowych. Infrastruktura ta obejmuje zarówno usługi ogólne, jak określono w art. 2 ust. 2 lit. e) rozporządzenia (UE) nr 283/2014, opracowane przez państwa członkowskie, jaki i platformę usług podstawowych, jak określono w art. 2 ust. 2 lit. d) tego rozporządzenia, opracowaną przez Komisję;

e) „inne wspólne europejskie usługi w dziedzinie e-zdrowia” oznaczają usługi cyfrowe, które można opracowywać w ramach sieci e-zdrowie i z których mogą wspólnie korzystać państwa członkowskie;

▼B

f) „model zarządzania” oznacza zestaw zasad dotyczących wyznaczania podmiotów uczestniczących w procesach podejmowania decyzji dotyczących europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia lub innych wspólnych europejskich usług w dziedzinie e-zdrowia opracowanych w ramach sieci e-zdrowie, a także opisu tych procesów;

▼M1

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 ([1]);

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;

([1]) 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).

▼M1

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.

▼B

2. Definicje zawarte w art. 4 pkt 1, 2, 7 i 8 rozporządzenia (UE) 2016/679 stosuje się odpowiednio.

Artykuł 3

Członkostwo w sieci e-zdrowie

1. Członkami sieci e-zdrowie są organy państw członkowskich odpowiedzialne za e-zdrowie, wyznaczone przez te państwa członkowskie, które uczestniczą w sieci e-zdrowie.

2. Państwa członkowskie pragnące uczestniczyć w sieci e-zdrowie powiadamiają Komisję na piśmie o:

a) decyzji o uczestnictwie w sieci e-zdrowie;

b) organie krajowym odpowiedzialnym za e-zdrowie, który zostanie członkiem sieci e-zdrowie, a także o imieniu i nazwisku przedstawiciela i jego zastępcy.

3. Członkowie powiadamiają na piśmie Komisję o:

a) decyzji o rezygnacji z członkostwa w sieci e-zdrowie;

b) wszelkich zmianach w informacjach, o których mowa w ust. 2 lit. b).

4. Komisja podaje do wiadomości publicznej wykaz członków uczestniczących w sieci e-zdrowie.

Artykuł 4

Działalność sieci e-zdrowie

1. Realizując cel, o którym mowa w art. 14 ust. 2 lit. a) dyrektywy 2011/24/UE, sieć e-zdrowie może w szczególności:

a) ułatwiać większą interoperacyjność krajowych systemów ICT oraz transgraniczną przenoszalność elektronicznych danych dotyczących zdrowia w transgranicznej opiece zdrowotnej;

b) zapewnić wytyczne dla państw członkowskich we współpracy z innymi właściwymi organami nadzoru w odniesieniu do wymiany danych dotyczących zdrowia między państwami członkowskimi oraz umożliwić obywatelom dostęp do własnych danych dotyczących zdrowia, jak również wymianę tych danych;

▼B

c) zapewnić wytyczne państwom członkowskim i ułatwić wymianę dobrych praktyk dotyczących rozwoju różnych cyfrowych usług w zakresie opieki zdrowotnej, takich jak telemedycyna, m-zdrowie lub nowe technologie w obszarze dużych zbiorów danych i sztucznej inteligencji, uwzględniając aktualnie prowadzone działania na szczeblu unijnym;

d) zapewnić wytyczne państwom członkowskim pod względem wspierania promocji zdrowia, zapobiegania chorobom oraz poprawy świadczenia usług opieki zdrowotnej dzięki lepszemu wykorzystaniu danych dotyczących zdrowia oraz podnoszeniu umiejętności cyfrowych pacjentów i pracowników służby zdrowia;

e) zapewnić wytyczne państwom członkowskim i ułatwić dobrowolną wymianę najlepszych praktyk dotyczących inwestowania w infrastrukturę cyfrową;

f) zapewnić państwom członkowskim wytyczne – we współpracy z innymi odpowiednimi podmiotami i zainteresowanymi stronami – w odniesieniu do przypadków zastosowań niezbędnych do interoperacyjności klinicznej oraz narzędzi służących jej osiągnięciu;

g) zapewnić członkom wytyczne dotyczące bezpieczeństwa europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia lub innych wspólnych europejskich usług w dziedzinie e-zdrowia opracowanych w ramach sieci e-zdrowie, uwzględniając prawodawstwo i dokumenty opracowane na szczeblu unijnym, zwłaszcza w obszarze bezpieczeństwa, a także zalecenia w dziedzinie cyberbezpieczeństwa, ściśle współpracując z grupą współpracy ds. bezpieczeństwa sieci i informacji oraz z Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji, a także, w stosownych przypadkach, z organami krajowymi;

▼M1

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.

▼B

2. Przy opracowywaniu wytycznych w sprawie skutecznych metod umożliwiających wykorzystywanie informacji medycznych do celów zdrowia publicznego i badań naukowych, o których mowa w art. 14 ust. 2 lit. b) ppkt (ii) dyrektywy 2011/24/UE, sieć e-zdrowie uwzględnia wytyczne przyjęte przez Europejską Radę Ochrony Danych i w stosownych przypadkach konsultuje się z tą Radą. Wytyczne te mogą również dotyczyć informacji wymienianych za pośrednictwem europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia lub innych wspólnych europejskich usług w dziedzinie e-zdrowia.

Artykuł 5

Funkcjonowanie sieci e-zdrowie

1. Sieć e-zdrowie ustanawia własny regulamin wewnętrzny zwykłą większością głosów swoich członków.

2. Sieć e-zdrowie przyjmuje wieloletni program działania i instrument oceny jego realizacji.

▼B

3. Aby wykonać powierzone zadania, sieć e-zdrowie może powołać stałe podgrupy w odniesieniu do konkretnych zadań, zwłaszcza dotyczących europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia lub innych wspólnych europejskich usług w dziedzinie e-zdrowia opracowanych w ramach sieci e-zdrowie.

4. Sieć e-zdrowie może również tworzyć tymczasowe podgrupy, w tym z udziałem ekspertów, w celu zbadania konkretnych kwestii zgodnie z wyznaczonym przez siebie zakresem zadań. Podgrupy są rozwiązywane niezwłocznie po wypełnieniu swojego mandatu.

5. Gdy członkowie sieci e-zdrowie postanowią rozwijać współpracę w niektórych obszarach objętych zakresem zadań sieci e-zdrowie, powinni uzgodnić zasady zaawansowanej współpracy i ich przestrzegać.

6. Realizując swoje cele, sieć e-zdrowie działa w ścisłej współpracy ze wspólnymi działaniami wspierającymi działania sieci e-zdrowie – w przypadku gdy takie wspólne działania istnieją – z zainteresowanymi stronami lub innymi zainteresowanymi podmiotami bądź mechanizmami wspierającymi oraz uwzględnia wyniki osiągnięte w ramach tych działań.

7. Sieć e-zdrowie opracowuje wraz z Komisją modele zarządzania europejską infrastrukturą usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia i uczestniczy w tym zarządzaniu poprzez:

(i) uzgadnianie priorytetów europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia oraz nadzorowanie ich wdrażania;

(ii) sporządzanie wytycznych i wymogów dotyczących działania, w tym wybór norm stosowanych w odniesieniu do europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia;

(iii) ustalanie, czy członkowie sieci e-zdrowie powinni mieć możliwość rozpoczęcia i kontynuowania wymiany elektronicznych danych dotyczących zdrowia poprzez europejską infrastrukturę usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia za pośrednictwem krajowych punktów kontaktowych ds. e-zdrowia, w oparciu o zgodność tych członków z wymogami ustanowionymi przez sieć e-zdrowie, ocenioną w ramach badań i audytów przeprowadzonych przez Komisję;

(iv) zatwierdzanie rocznego planu prac dotyczącego europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia.

8. Sieć e-zdrowie może opracować wraz z Komisją modele zarządzania innymi wspólnymi europejskimi usługami w dziedzinie e-zdrowia opracowanymi w ramach sieci e-zdrowie, a także uczestniczyć w zarządzaniu tymi usługami. Sieć, wraz z Komisją, może także wyznaczyć priorytety oraz sporządzić wytyczne dotyczące funkcjonowania takich wspólnych europejskich usług w dziedzinie e-zdrowia.

▼B

9. Regulamin wewnętrzny może przewidywać, że państwa inne niż państwa członkowskie, stosujące dyrektywę 2011/24/UE, mogą uczestniczyć w posiedzeniach sieci e-zdrowie w roli obserwatorów.

10. Członkowie sieci e-zdrowie i ich przedstawiciele oraz zaproszeni eksperci i obserwatorzy podlegają obowiązkom zachowania tajemnicy zawodowej określonym w art. 339 Traktatu, a także przepisom Komisji dotyczącym bezpieczeństwa w zakresie ochrony informacji niejawnych UE, określonym w decyzji Komisji (UE, Euratom) 2015/444 ([1]). Jeżeli nie będą przestrzegać tych obowiązków, przewodniczący sieci e-zdrowie może zastosować wszystkie odpowiednie środki, o których mowa w regulaminie wewnętrznym.

Artykuł 6

Powiązania między siecią e-zdrowie a Komisją

1. Komisja:

a) bierze udział w posiedzeniach sieci e-zdrowie wraz z przedstawicielem członków i współprzewodniczy tym posiedzeniom;

b) współpracuje z siecią e-zdrowie w odniesieniu do jej działań i udziela jej wsparcia;

c) zapewnia obsługę sekretariatu sieci e-zdrowie;

d) opracowuje, wdraża i utrzymuje odpowiednie środki techniczne i organizacyjne dotyczące usług podstawowych europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia;

e) wspiera sieć e-zdrowie w stwierdzaniu technicznej i organizacyjnej zgodności krajowych punktów kontaktowych ds. e-zdrowia z wymogami dotyczącymi transgranicznej wymiany danych dotyczących zdrowia, zapewniając i przeprowadzając niezbędne badania i audyty. Eksperci z państw członkowskich mogą wspierać audytorów Komisji;

▼M1

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.

▼B

2. Komisja może uczestniczyć w posiedzeniach podgrup sieci e-zdrowie.

3. Komisja może konsultować się z siecią e-zdrowie w kwestiach dotyczących e-zdrowia na szczeblu unijnym oraz w kwestiach dotyczących wymiany najlepszych praktyk w dziedzinie e-zdrowia.

([1]) Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 72 z 17.3.2015, s. 53).

▼B

4. Komisja podaje do wiadomości publicznej informacje na temat działań prowadzonych przez sieć e-zdrowie.

Artykuł 7

▼M1

Ochrona danych osobowych przetwarzanych za pośrednictwem europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia

▼B

1. Państwa członkowskie, reprezentowane przez odpowiednie organy krajowe lub inne wyznaczone podmioty, traktuje się jako administratorów danych osobowych, które przetwarzają za pośrednictwem europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia; państwa członkowskie w jasny i przejrzysty sposób przydzielają obowiązki administratorom.

2. Komisję uznaje się za podmiot przetwarzający dane osobowe pacjentów przetwarzane za pośrednictwem europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia. Jako podmiot przetwarzający Komisja zarządza usługami podstawowymi europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia i przestrzega obowiązków podmiotu przetwarzającego określonych w ►M1 załączniku I ◄ do niniejszej decyzji. Komisja nie ma dostępu do danych osobowych pacjentów przetwarzanych za pośrednictwem europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia.

3. Komisję uznaje się za administratora w procesie przetwarzania danych osobowych niezbędnych do przyznania praw dostępu do usług podstawowych europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia i zarządzania tymi prawami. Takimi danymi są dane kontaktowe użytkowników, m.in. imię, nazwisko i adres e-mail, a także ich przynależność do systemu ubezpieczeń.

▼M1

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.

▼M1

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.

▼B

Artykuł 8

Wydatki

1. Osoby uczestniczące w działaniach sieci e-zdrowie nie otrzymują od Komisji wynagrodzenia za swoją pracę.

▼B

2. Koszty podróży i koszty utrzymania ponoszone przez uczestników działań sieci e-zdrowie są zwracane przez Komisję zgodnie z obowiązującymi w ramach Komisji zasadami dotyczącymi zwrotu kosztów poniesionych przez osoby niebędące pracownikami Komisji zaproszone do udziału w posiedzeniach w charakterze ekspertów. Zwrot tych kosztów odbywa się w granicach dostępnych środków finansowych przyznanych w ramach rocznej procedury przydziału zasobów.

Artykuł 9

Uchylenie

Decyzja wykonawcza 2011/890/UE traci moc. Odesłania do uchylonej decyzji odczytuje się jako odesłania do niniejszej decyzji.

Artykuł 10

Adresaci

Niniejsza decyzja skierowana jest do państw członkowskich.

▼M1

ZAŁĄCZNIK I

▼B

OBOWIĄZKI KOMISJI JAKO PODMIOTU PRZETWARZAJĄCEGO DANE W ODNIESIENIU DO EUROPEJSKIEJ INFRASTRUKTURY USŁUG CYFROWYCH W DZIEDZINIE E-ZDROWIA W ZAKRESIE TRANSGRANICZNYCH USŁUG INFORMACYJNYCH W DZIEDZINIE E-ZDROWIA

Komisja:

1. Tworzy i zapewnia bezpieczną i niezawodną infrastrukturę łączności, która łączy ze sobą sieci członków sieci e-zdrowie zaangażowanych w europejską infrastrukturę usług cyfrowych w dziedzinie e-zdrowia w zakresie transgranicznych usług informacyjnych w dziedzinie e-zdrowia („centralna bezpieczna infrastruktura łączności"). Aby wywiązać się ze swoich obowiązków, Komisja może zaangażować osoby trzecie. Komisja zapewnia, aby do tych osób trzecich zastosowanie miały takie same obowiązki dotyczące ochrony danych jak te określone w niniejszej decyzji.

2. Konfiguruje część centralnej bezpiecznej infrastruktury łączności w taki sposób, aby krajowe punkty kontaktowe ds. e-zdrowia mogły prowadzić wymianę informacji w sposób bezpieczny, niezawodny i skuteczny.

3. Komisja przetwarza dane osobowe zgodnie z udokumentowanymi instrukcjami administratorów.

4. Wprowadza wszystkie organizacyjne, fizyczne i logiczne środki bezpieczeństwa służące utrzymaniu centralnej bezpiecznej infrastruktury łączności. W tym celu Komisja:

   a) wyznacza podmiot odpowiedzialny za zarządzanie bezpieczeństwem na poziomie centralnej bezpiecznej infrastruktury łączności, przekazuje administratorom danych informacje kontaktowe oraz zapewnia ich dostępność w celu reagowania na zagrożenia dla bezpieczeństwa;

   b) przyjmuje odpowiedzialność za bezpieczeństwo centralnej bezpiecznej infrastruktury łączności;

   c) zapewnia, aby wszystkie osoby, które otrzymają dostęp do centralnej bezpiecznej infrastruktury łączności, podlegały umownemu, zawodowemu lub ustawowemu obowiązkowi zachowania poufności;

   d) zapewnia, aby personel posiadający dostęp do informacji niejawnych spełniał odpowiednie kryteria stosowane w celu uzyskania poświadczenia bezpieczeństwa i kryteria poufności.

5. Wprowadza wszystkie niezbędne środki bezpieczeństwa, aby nie dopuścić do zakłócenia sprawnego funkcjonowania operacyjnego drugiej domeny. W tym celu Komisja wprowadza szczególne procedury związane z połączeniem z centralną bezpieczną infrastrukturą łączności. Informacje te dotyczą:

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

   b) procedury audytu i przeglądu, aby:

      (i) sprawdzać zgodność między wprowadzonymi środkami bezpieczeństwa a stosowaną polityką 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 wyeliminowanie istniejących uchybień w zakresie bezpieczeństwa; oraz

▼B

(v) określić warunki, na jakich należy udzielać zezwoleń, w tym na wniosek administratorów, oraz przyczyniać się do przeprowadzania niezależnych audytów, w tym inspekcji i przeglądów środków bezpieczeństwa;

c) procedury kontroli zmian, by udokumentować i zmierzyć wpływ zmiany przed jej wdrożeniem oraz na bieżąco informować krajowe punkty kontaktowe ds. e-zdrowia o wszelkich zmianach, które mogą wpłynąć na łączność z pozostałymi krajowymi infrastrukturami lub na ich bezpieczeństwo;

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

e) procedury dotyczącej cyberincydentu, by określić system zgłaszania i eskalacji, bezzwłocznie poinformować odpowiedzialną administrację krajową oraz Europejskiego Inspektora Ochrony Danych o wszelkich naruszeniach bezpieczeństwa, a także określić procedurę dyscyplinarną w przypadku naruszeń bezpieczeństwa.

6. Wprowadza fizyczne lub logiczne środki bezpieczeństwa w odniesieniu do obiektów, w których znajduje się sprzęt centralnej bezpiecznej infrastruktury łączności, 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, które otrzymały dostęp do obiektów, towarzyszył odpowiednio upoważniony personel właściwej organizacji;

d) zapewnia, aby sprzęt nie mógł zostać dodany, wymieniony ani usunięty bez uprzedniej zgody wyznaczonych odpowiedzialnych podmiotów;

e) kontroluje dostęp z oraz do innej sieci lub innych sieci wzajemnie połączonych z centralną bezpieczną infrastrukturą łączności;

f) zapewnia, aby osoby, które uzyskują dostęp do centralnej bezpiecznej infrastruktury łączności, zostały zidentyfikowane i uwierzytelnione;

g) dokonuje przeglądu uprawnień do udzielania zezwoleń na dostęp do centralnej bezpiecznej infrastruktury łączności w przypadku wykrycia naruszenia bezpieczeństwa mającego wpływ na tę infrastrukturę;

h) zachowuje integralność informacji przekazywanych za pośrednictwem centralnej bezpiecznej infrastruktury łączności;

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 centralnej bezpiecznej infrastruktury łączności z domeny krajowych punktów kontaktowych ds. e-zdrowia (tj. zablokowanie lokalizacji/adresu IP).

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

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

▼B

9. Monitoruje – w czasie rzeczywistym – wydajność wszystkich komponentów usług w ramach centralnej bezpiecznej infrastruktury łączności, tworzy regularne statystyki i prowadzi rejestry.

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

11. Wspiera administratorów poprzez przekazywanie im informacji na temat centralnej bezpiecznej infrastruktury łączności w ramach europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia w celu realizacji obowiązków przewidzianych w art. 35 i 36 rozporządzenia (UE) 2016/679.

12. Zapewnia, aby dane przekazywane za pośrednictwem centralnej bezpiecznej infrastruktury łączności były szyfrowane.

13. Wprowadza wszystkie odpowiednie środki, by zapobiec sytuacji, w której operatorzy centralnej bezpiecznej infrastruktury łączności mogliby uzyskać nieuprawniony dostęp do przekazywanych danych.

14. Wprowadza środki mające na celu ułatwienie interoperacyjności i łączności między wyznaczonymi krajowymi właściwymi administracjami centralnej bezpiecznej infrastruktury łączności.

▼M1

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

([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.

▼M1

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.

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.

▼M1

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:

▼M1

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 ([1]);

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:

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

▼M1

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.

▼**M1**

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.