Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2024/2639

10.10.2024

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2024/2639

z dnia 9 października 2024 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/988 w odniesieniu do ról i zadań pojedynczych krajowych punktów kontaktowych systemu wczesnego ostrzegania Safety Gate

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z dnia 10 maja 2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG ([1]), w szczególności jego art. 25 ust. 2 akapit drugi,

a także mając na uwadze, co następuje:

(1) Rozporządzenie (UE) 2023/988 stanowi, że system wczesnego ostrzegania Safety Gate jest systemem wczesnego ostrzegania służącym wymianie informacji na temat środków naprawczych w zakresie produktów niebezpiecznych. Aby zapewnić skuteczny przepływ informacji i właściwe funkcjonowanie systemu wczesnego ostrzegania Safety Gate, zgodnie z art. 25 ust. 2 akapit pierwszy rozporządzenia (UE) 2023/988, każde państwo członkowskie jest zobowiązane wyznaczyć pojedynczy krajowy punkt kontaktowy dla systemu wczesnego ostrzegania Safety Gate („punkt kontaktowy Safety Gate"). Zgodnie z art. 25 ust. 2 akapit pierwszy rozporządzenia (UE) 2023/988 punkt kontaktowy Safety Gate jest odpowiedzialny przynajmniej za sprawdzanie kompletności zgłoszeń przedłożonych do zatwierdzenia przez Komisję, a także za komunikację z Komisją w zakresie zadań przewidzianych w art. 26 ust. 1–6 tego rozporządzenia. Wyznaczenie krajowego punktu kontaktowego Safety Gate powinno pozostawać bez uszczerbku dla kompetencji państw członkowskich w zakresie organizacji ich systemów nadzoru rynku.

(2) W decyzji wykonawczej Komisji (UE) 2019/417 ([2]) ustanowiono wytyczne dotyczące zarządzania unijnym systemem szybkiej informacji („RAPEX") utworzonym na mocy uchylonej dyrektywy 2001/95/WE Parlamentu Europejskiego i Rady ([3]). W tej decyzji wykonawczej określono zadania krajowych punktów kontaktowych RAPEX, w tym zadania polegające na organizowaniu pracy właściwych organów krajowych i kierowaniu nią, dopilnowaniu prawidłowego wykonywania wszystkich zadań, w szczególności aby wszystkie wymagane informacje były przekazywane Komisji bez opóźnień, oraz koordynowaniu wszystkich krajowych działań i inicjatyw związanych z systemem. Biorąc pod uwagę dobre doświadczenia związane z funkcjonowaniem krajowych punktów kontaktowych RAPEX, role i zadania punktów kontaktowych Safety Gate powinny w stosownych przypadkach obejmować role i zadania określone w decyzji wykonawczej (UE) 2019/417.

(3) Aby zapewnić skuteczny przepływ informacji między punktem kontaktowym Safety Gate a różnymi organami uczestniczącymi w systemie wczesnego ostrzegania Safety Gate w danym państwie członkowskim, punkt kontaktowy Safety Gate powinien organizować pracę sieci przyporządkowanych do niego organów krajowych zajmujących się systemem wczesnego ostrzegania Safety Gate („krajowa sieć Safety Gate") oraz nią kierować.

(4) Zgodnie ze swoimi zadaniami wynikającymi z decyzji wykonawczej (UE) 2019/417 oraz w celu zapewnienia efektywnego wykorzystania systemu wczesnego ostrzegania Safety Gate, a także spójności przekazywanych informacji punkty kontaktowe Safety Gate powinny szkolić organy krajowe i pomagać im w korzystaniu z tego systemu.

([1]) Dz.U. L 135 z 23.5.2023, s. 1, ELI: http://data.europa.eu/eli/reg/2023/988/oj.

([2]) Decyzja wykonawcza Komisji (UE) 2019/417 z dnia 8 listopada 2018 r. ustanawiająca wytyczne dotyczące zarządzania unijnym systemem szybkiej informacji RAPEX utworzonym na mocy art. 12 dyrektywy 2001/95/WE w sprawie ogólnego bezpieczeństwa produktów oraz funkcjonującym w jego ramach systemem zgłoszeń (Dz.U. L 73 z 15.3.2019, s. 121, ELI: http://data.europa.eu/eli/dec/2019/417/oj).

([3]) Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz.U. L 11 z 15.1.2002, s. 4, ELI: http://data.europa.eu/eli/dir/2001/95/oj).

(5) Aby uniknąć powielania zgłoszeń w systemie wczesnego ostrzegania Safety Gate, punkty kontaktowe Safety Gate powinny przed dokonaniem zgłoszenia sprawdzać, w stosownych przypadkach z udziałem organów krajowych, czy środek dotyczący danego produktu został już zgłoszony w systemie wczesnego ostrzegania Safety Gate.

(6) Opracowany i zarządzany przez Komisję system informatyczny „eSurveillance Webcrawler – Bezpieczeństwo produktów" ma na celu wykrywanie produktów, które zostały zgłoszone w systemie wczesnego ostrzegania Safety Gate i są nadal sprzedawane lub ponownie wprowadzane do obrotu w sklepach internetowych i na internetowych platformach handlowych. Aby zwiększyć skuteczność nadzoru rynku online, jego stosowanie powinno być szeroko promowane, w stosownych przypadkach wraz z innymi podobnymi narzędziami stosowanymi przez organy.

(7) Komisja i organy krajowe działają jako współadministratorzy danych w systemie wczesnego ostrzegania Safety Gate zgodnie z art. 26 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([4]) i art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([5]). Należy zatem określić role i obowiązki poszczególnych współadministratorów.

(8) Niniejsze rozporządzenie należy stosować od tej samej daty co rozporządzenie (UE) 2023/988.

(9) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią Komitetu ds. Rozporządzenia w sprawie Ogólnego Bezpieczeństwa Produktów ustanowionego na mocy art. 46 ust. 1 rozporządzenia (UE) 2023/988,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Rola i zadania pojedynczych krajowych punktów kontaktowych zgodnie z art. 25 ust. 2 rozporządzenia (UE) 2023/988 („punkty kontaktowe Safety Gate") są następujące:

a) weryfikacja i walidacja kompletności powiadomień otrzymanych od innych organów krajowych w ich państwie członkowskim przed przekazaniem ich Komisji za pośrednictwem systemu wczesnego ostrzegania Safety Gate zgodnie z art. 25 ust. 2 akapit pierwszy rozporządzenia (UE) 2023/988;

b) sprawdzanie, przed dokonaniem zgłoszenia za pośrednictwem systemu wczesnego ostrzegania Safety Gate, czy produkt będący przedmiotem tego powiadomienia został już zgłoszony w tym systemie, a jeśli tak – przedkładanie zgłoszeń uzupełniających zgodnie z art. 26 ust. 7 rozporządzenia (UE) 2023/988, w stosownych przypadkach we współpracy z właściwym organem krajowym;

c) zapewnienie, aby zgłoszenia innych państw członkowskich, które zostały zatwierdzone przez Komisję, w systemie wczesnego ostrzegania Safety Gate docierały do odpowiednich organów krajowych, w tym organów odpowiedzialnych za kontrole na granicach zewnętrznych, w ich państwie członkowskim, w celu podjęcia odpowiednich działań następczych na szczeblu krajowym;

d) promowanie stosowania systemu eSurveillance Webcrawler dotyczącego bezpieczeństwa produktów oraz w stosownych przypadkach innych podobnych narzędzi w danym państwie członkowskim, a w szczególności podejmowania przez organy krajowe działań następczych w związku z wynikami działania tego systemu;

e) szkolenie i wspieranie wszystkich organów krajowych w korzystaniu z systemu wczesnego ostrzegania Safety Gate;

([4]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

f) ułatwianie wykonywania w ich państwie członkowskim zadań związanych z systemem wczesnego ostrzegania Safety Gate wynikających z rozporządzenia (UE) 2023/988 i rozporządzenia delegowanego Komisji z dnia 27 sierpnia 2024 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 w zakresie zasad dostępu do systemu wczesnego ostrzegania Safety Gate i jego działania, informacji, które mają być do niego wprowadzane, wymagań dotyczących zgłoszeń oraz kryteriów oceny poziomu ryzyka ([6]), a w szczególności zapewnienie przekazywania Komisji wszystkich wymaganych informacji zgodnie z rozporządzeniem (UE) 2023/988;

g) współpraca i wymiana informacji istotnych dla bezpieczeństwa produktów z innymi punktami kontaktowymi Safety Gate oraz uczestnictwo w dyskusjach między punktami kontaktowymi Safety Gate, koordynowanych przez Komisję;

h) wymiana informacji istotnych dla bezpieczeństwa produktów na szczeblu krajowym z organem, który jest członkiem Sieci ds. Bezpieczeństwa Konsumentów, o której mowa w art. 30 rozporządzenia (UE) 2023/988, w przypadku gdy jest to inny organ niż punkt kontaktowy Safety Gate;

i) wymiana informacji istotnych dla bezpieczeństwa produktów na szczeblu krajowym z jednolitym urzędem łącznikowym wyznaczonym na podstawie art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 ([7]) i art. 23 ust. 1 rozporządzenia (UE) 2023/988, jeżeli jest to inny organ niż punkt kontaktowy Safety Gate;

j) niezwłoczne informowanie Komisji o wszelkich problemach technicznych związanych z funkcjonowaniem systemu wczesnego ostrzegania Safety Gate;

k) zarządzanie wnioskami o dostęp do aplikacji związanych z systemem wczesnego ostrzegania Safety Gate otrzymanymi od użytkowników w ich krajowej sieci Safety Gate oraz informowanie Komisji o wszelkich zmianach dotyczących pracowników, które mają wpływ na prawa dostępu;

l) odpowiadanie na wnioski dotyczące funkcjonowania systemu wczesnego ostrzegania Safety Gate w danym państwie członkowskim, otrzymane od zainteresowanych stron, w tym podmiotów gospodarczych i dostawców internetowych platform handlowych;

m) w stosownych przypadkach kontaktowanie się z organem w danym państwie członkowskim, który przedłożył dane zgłoszenie w systemie wczesnego ostrzegania Safety Gate, w sprawie ewentualnego uzupełnienia tego zgłoszenia o dodatkowe informacje na wniosek podmiotów gospodarczych lub dostawców internetowych platform handlowych, w szczególności gdy niekompletny charakter zgłoszenia w systemie wczesnego ostrzegania Safety Gate może mieć negatywny wpływ na te przedsiębiorstwa.

Artykuł 2

Role i obowiązki Komisji i organów krajowych jako współadministratorów danych w systemie wczesnego ostrzegania Safety Gate zgodnie z art. 26 rozporządzenia (UE) 2016/679 i art. 28 rozporządzenia (UE) 2018/1725 określono w załączniku do niniejszego rozporządzenia.

([6]) Dotychczas nieopublikowane w Dzienniku Urzędowym.

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.U. L 169 z 25.6.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/1020/oj).

Artykuł 3

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie stosuje się od dnia 13 grudnia 2024 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 9 października 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

WSPÓŁADMINISTROWANIE SYSTEMEM WCZESNEGO OSTRZEGANIA SAFETY GATE

1. PRZEDMIOT I OPIS PRZETWARZANIA

System wczesnego ostrzegania Safety Gate to system powiadamiania obsługiwany przez Komisję, który służy do szybkiej wymiany informacji między organami krajowymi państw członkowskich, organami trzech państw Europejskiego Obszaru Gospodarczego/Europejskiego Stowarzyszenia Wolnego Handlu (EOG/EFTA) (Islandia, Liechtenstein i Norwegia) oraz Komisją na temat środków zastosowanych w odniesieniu do produktów niebezpiecznych wykrytych na rynku Unii lub EOG/EFTA.

System ma umożliwiać szybką wymianę informacji na temat środków naprawczych podjętych w całej Unii w odniesieniu do produktów stwarzających zagrożenie.

Wymiana informacji dotyczy środków naprawczych wprowadzonych w odniesieniu do niebezpiecznych produktów konsumenckich i produktów dla profesjonalistów, objętych zakresem rozporządzeń (UE) 2023/988 lub (UE) 2019/1020.

System wczesnego ostrzegania Safety Gate obejmuje zarówno środki nakazane przez organy krajowe, jak i środki podejmowane dobrowolnie przez podmioty gospodarcze.

2. ZAKRES WSPÓŁADMINISTROWANIA

Komisja i organy krajowe działają jako współadministratorzy przetwarzania danych w systemie wczesnego ostrzegania Safety Gate. „Organy krajowe" oznaczają wszystkie organy działające w zakresie bezpieczeństwa produktów w państwach członkowskich lub państwach EFTA/EOG oraz uczestniczące w unijnej sieci punktów kontaktowych Safety Gate, w tym organy nadzoru rynku odpowiedzialne za monitorowanie zgodności produktów z wymogami bezpieczeństwa oraz organy odpowiedzialne za kontrole granic zewnętrznych.

Do celów art. 26 rozporządzenia (UE) 2016/679 i art. 28 rozporządzenia (UE) 2018/1725 Komisja jako współadministrator danych osobowych jest odpowiedzialna za następujące czynności przetwarzania:

1) przetwarzanie przez Komisję informacji dotyczących środków wprowadzonych względem produktów stwarzających poważne zagrożenie, przywożonych do Unii i Europejskiego Obszaru Gospodarczego lub z nich wywożonych, w celu przekazania tych informacji pojedynczym krajowym punktom kontaktowym systemu wczesnego ostrzegania Safety Gate („punkty kontaktowe Safety Gate");

2) przetwarzanie przez Komisję informacji otrzymanych od państw trzecich, organizacji międzynarodowych, przedsiębiorstw lub innych systemów wczesnego ostrzegania, dotyczących produktów stwarzających zagrożenie dla zdrowia i bezpieczeństwa konsumentów, które pochodzącą z UE i spoza UE, w celu przekazania tych informacji organom krajowym.

Wykonując te działania, Komisja zapewnia przestrzeganie mających zastosowanie obowiązków i warunków określonych w rozporządzeniu (UE) 2018/1725.

Do kompetencji organów krajowych jako współadministratorów danych osobowych należą następujące czynności przetwarzania:

1) przetwarzanie przez organy krajowe informacji na podstawie art. 26 rozporządzenia (UE) 2023/988 w sprawie ogólnego bezpieczeństwa produktów i art. 20 rozporządzenia (UE) 2019/1020 w celu przekazania takich informacji Komisji i państwom członkowskim oraz państwom EFTA/EOG;

2) przetwarzanie przez organy krajowe informacji wynikających z ich działań następczych przeprowadzonych w związku ze zgłoszeniami w systemie wczesnego ostrzegania Safety Gate w celu przekazania tych informacji Komisji i państwom członkowskim oraz państwom EFTA/EOG.

Wykonując te działania, organy krajowe zapewniają przestrzeganie mających zastosowanie obowiązków i warunków określonych w rozporządzeniu (UE) 2016/679.

3. OBOWIĄZKI, ROLE I RELACJE WSPÓŁADMINISTRATORÓW W STOSUNKU DO OSÓB, KTÓRYCH DANE DOTYCZĄ

3.1. **Kategorie osób, których dane dotyczą, i danych osobowych**

Współadministratorzy wspólnie przetwarzają następujące kategorie danych osobowych:

a) Dane kontaktowe użytkowników systemu wczesnego ostrzegania Safety Gate.

Przetwarzane mogą być następujące dane dotyczące użytkowników systemu wczesnego ostrzegania Safety Gate:

— imię,

— nazwisko,

— adres e-mail,

— kraj,

— preferowany język.

b) Dane kontaktowe osób lub organów będących autorami lub zatwierdzających zgłoszenia i uwagi przekazane za pośrednictwem systemu wczesnego ostrzegania Safety Gate.

Do osób lub organów będących autorami lub zatwierdzających zgłoszenia i uwagi należą:

— punkty kontaktowe Safety Gate oraz inspektorzy z organów nadzoru rynku państw członkowskich i państw EFTA/EOG lub z krajowych organów odpowiedzialnych za kontrole granic zewnętrznych, którzy uczestniczą w procedurze zgłoszeniowej;

— pracownicy Komisji, w tym urzędnicy, pracownicy zatrudnieni na czas określony, pracownicy kontraktowi, stażyści i usługodawcy zewnętrzni.

Przetwarzane mogą być następujące dane osób lub organów będących autorami lub zatwierdzających zgłoszenia i uwagi przekazane za pośrednictwem systemu wczesnego ostrzegania Safety Gate:

— imię,

— nazwisko,

— nazwa organu,

— adres,

— adres e-mail,

— numer telefonu.

c) Ponadto w systemie wczesnego ostrzegania Safety Gate mogą dodatkowo zostać ujęte dwa rodzaje danych osobowych:

(i) Kiedy konieczne jest wykrycie produktów niebezpiecznych zdefiniowanych w art. 3 pkt 3 rozporządzenia (UE) 2023/988, dane kontaktowe podmiotów gospodarczych mogą zawierać dane osobowe, które zostaną włączone do systemu wczesnego ostrzegania Safety Gate. Takie dane są wprowadzane do systemu wczesnego ostrzegania Safety Gate wyłącznie przez organy krajowe na podstawie informacji zgromadzonych podczas dochodzenia. Przetwarzane mogą być następujące dane podmiotów gospodarczych:

— nazwa,

— adres,

— miejscowość,

— kraj,

— dane kontaktowe ([1]),

([1]) To pole może odnosić się do osoby fizycznej reprezentującej producentów lub upoważnionych przedstawicieli. Państwa członkowskie są jednak proszone o unikanie wprowadzania jakichkolwiek danych osobowych i korzystanie głównie z nieosobowych danych kontaktowych, takich jak ogólne adresy e-mail;

— adres kontaktowy.

(ii) Imiona i nazwiska osób, które przeprowadziły badania produktów niebezpiecznych i/lub uwierzytelniły sprawozdania z badań – o ile ich imiona i nazwiska zostały one dodatkowo ujęte w innych dokumentach, np. w sprawozdaniach z badań.

3.2. **Przekazywanie informacji osobom, których dane dotyczą**

Komisja podaje informacje, o których mowa w art. 15 i 16, oraz przekazuje wszelkie komunikaty na mocy art. 17–24 i 35 rozporządzenia (UE) 2018/1725 w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Komisja podejmuje również odpowiednie środki, aby pomóc organom krajowym w podawaniu informacji, o których mowa w art. 13 i 14, oraz przekazywaniu wszelkich komunikatów na mocy art. 19–26 i 37 rozporządzenia (UE) 2016/679 w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, na temat następujących danych:

— dane dotyczące użytkowników systemu wczesnego ostrzegania Safety Gate;

— dane dotyczące autorów zgłoszeń i uwag oraz osób je zatwierdzających.

Użytkowników systemu wczesnego ostrzegania Safety Gate informuje się o przysługujących im prawach za pośrednictwem oświadczenia o ochronie prywatności dostępnego w systemie wczesnego ostrzegania Safety Gate.

Organy krajowe podejmują odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem podawać wszelkie informacje, o których mowa w art. 13 i 14, oraz przekazywać wszelkie komunikaty na mocy art. 19–26 i 37 rozporządzenia (UE) 2016/679 dotyczące następujących danych:

— informacje o osobach prawnych, które identyfikują osobę fizyczną

— imiona i nazwiska oraz inne dane osób, które przeprowadziły badania produktów niebezpiecznych lub uwierzytelniły sprawozdania z badań.

Informacje przekazuje się na piśmie, w tym drogą elektroniczną.

Przy wypełnianiu swoich obowiązków dotyczących osób, których dane dotyczą, organy krajowe stosują wzór oświadczenia o ochronie prywatności udostępniony przez Komisję.

3.3. **Rozpatrywanie wniosków osób, których dane dotyczą**

Osoby, których dane dotyczą, mogą wykonywać swoje prawa wynikające z rozporządzenia (UE) 2018/1725 i rozporządzenia (UE) 2016/679 odpowiednio w odniesieniu do Komisji lub organów krajowych pełniących funkcję współadministratorów.

Współadministratorzy rozpatrują wnioski osób, których dane dotyczą, zgodnie z procedurą ustanowioną w tym celu przez współadministratorów. Szczegółową procedurę wykonywania praw osób, których dane dotyczą, wyjaśniono w oświadczeniu o ochronie prywatności.

Współadministratorzy współpracują ze sobą i na wniosek udzielają sobie wzajemnie szybkiej i skutecznej pomocy w rozpatrywaniu wszelkich wniosków osób, których dane dotyczą.

Jeżeli jeden ze współadministratorów otrzyma wniosek osoby, której dane dotyczą, a którego rozpatrzenie nie należy do jego obowiązków, współadministrator ten niezwłocznie, a najpóźniej w ciągu siedmiu dni kalendarzowych od otrzymania wniosku, przekazuje go współadministratorowi faktycznie odpowiedzialnemu za jego rozpatrzenie. W ciągu kolejnych trzech dni kalendarzowych od otrzymania przekazanego wniosku odpowiedzialny współadministrator wysyła potwierdzenie otrzymania wniosku do osoby, której dane dotyczą, informując jednocześnie o tym współadministratora, który otrzymał wniosek w pierwszej kolejności.

W odpowiedzi na wniosek osoby, której dane dotyczą, o dostęp do danych osobowych żaden ze współadministratorów nie ujawnia ani w inny sposób nie udostępnia żadnych danych osobowych przetwarzanych wspólnie bez uprzedniej konsultacji z drugim współadministratorem.

4. INNE OBOWIĄZKI I ROLE WSPÓŁADMINISTRATORÓW

4.1. **Bezpieczeństwo przetwarzania danych**

Każdy współadministrator wdraża odpowiednie środki techniczne i organizacyjne mające na celu:

a) zapewnienie i ochronę bezpieczeństwa, integralności i poufności wspólnie przetwarzanych danych osobowych zgodnie z decyzją Komisji (UE, Euratom) 2017/46 ([2]) i właściwym aktem prawnym – odpowiednio – państwa członkowskiego UE lub państwa EFTA/EOG;

b) ochronę danych osobowych będących w jego posiadaniu przed wszelkiego rodzaju przetwarzaniem, utratą, wykorzystaniem, ujawnieniem lub nabyciem, które jest nieuprawnione lub niezgodne z prawem, lub przed nieuprawnionym lub niezgodnym z prawem dostępem do tych danych;

c) nieujawnianie ani niezezwalanie na dostęp do danych osobowych innej osobie niż uprzednio uzgodnieni odbiorcy lub podmioty przetwarzające.

Każdy współadministrator wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa przetwarzania zgodnie z – odpowiednio – art. 33 rozporządzenia (UE) 2018/1725 i art. 32 rozporządzenia (UE) 2016/679.

Współadministratorzy udzielają sobie wzajemnie szybkiej i skutecznej pomocy w przypadku cyberincydentów, w tym naruszeń ochrony danych osobowych.

4.2. **Zarządzanie cyberincydentami, w tym naruszeniami ochrony danych osobowych**

Współadministratorzy zajmują się cyberincydentami, w tym przypadkami naruszenia ochrony danych osobowych, zgodnie ze swoimi procedurami wewnętrznymi i obowiązującymi przepisami.

Współadministratorzy w szczególności udzielają sobie wzajemnie szybkiej i skutecznej pomocy niezbędnej do ułatwienia identyfikacji wszelkich cyberincydentów związanych z operacją wspólnego przetwarzania, w tym przypadków naruszeń ochrony danych osobowych, oraz do określenia procedur postępowania w przypadku takich incydentów.

Administratorzy powiadamiają się wzajemnie o następujących kwestiach:

a) wszelkim potencjalnym lub faktycznym ryzyku dla dostępności, poufności lub integralności danych osobowych podlegających wspólnemu przetwarzaniu;

b) wszelkich cyberincydentach, które mają związek z operacją wspólnego przetwarzania;

c) wszelkich przypadkach naruszenia ochrony danych osobowych (tj. wszelkich naruszeniach bezpieczeństwa prowadzących do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych podlegających wspólnemu przetwarzaniu), możliwych konsekwencjach naruszenia ochrony danych osobowych oraz ocenie ryzyka dla praw i wolności osób fizycznych, a także wszelkich działaniach podjętych w celu zaradzenia naruszeniu ochrony danych osobowych i zminimalizowania ryzyka naruszenia praw lub wolności osób fizycznych;

d) wszelkich naruszeniach zabezpieczeń technicznych lub organizacyjnych operacji wspólnego przetwarzania.

Każdy ze współadministratorów jest odpowiedzialny za postępowanie w przypadku wszelkich cyberincydentów, w tym naruszeń ochrony danych osobowych, do których dochodzi w wyniku naruszenia zobowiązań danego współadministratora wynikających z niniejszego rozporządzenia wykonawczego oraz odpowiednio rozporządzenia (UE) 2018/1725 i rozporządzenia (UE) 2016/679.

Współadministratorzy dokumentują cyberincydenty (w tym naruszenia ochrony danych osobowych) i powiadamiają się wzajemnie bez zbędnej zwłoki, a najpóźniej w ciągu 48 godzin od uzyskania informacji o cyberincydencie (w tym o naruszeniu ochrony danych osobowych).

Współadministrator odpowiedzialny za naruszenie ochrony danych osobowych dokumentuje i zgłasza je Europejskiemu Inspektorowi Ochrony Danych lub właściwemu krajowemu organowi nadzorczemu. Współadministrator dokonuje zgłoszenia bez zbędnej zwłoki – w miarę możliwości nie później niż 72 godziny po uzyskaniu informacji o naruszeniu ochrony danych osobowych –, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Współadministrator odpowiedzialny informuje o takim zgłoszeniu drugiego współadministratora.

Współadministrator odpowiedzialny za naruszenie ochrony danych osobowych powiadamia o tym naruszeniu zainteresowane osoby, których dane dotyczą, jeśli takie naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Współadministrator odpowiedzialny informuje o takim powiadomieniu drugiego współadministratora.

([2]) 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, ELI: http://data.europa.eu/eli/dec/2017/46/oj).

4.3. **Lokalizacja danych osobowych**

Dane osobowe gromadzone do celów procesu powiadamiania za pośrednictwem systemu wczesnego ostrzegania Safety Gate przechowuje i gromadzi się w systemie wczesnego ostrzegania Safety Gate w celu zapewnienia, aby dostęp do aplikacji był ograniczony wyłącznie do wyraźnie określonych osób, a tym samym aby dane przechowywane w tej aplikacji były dobrze chronione.

Dane osobowe zgromadzone do celów operacji przetwarzania przetwarza się wyłącznie na terytorium UE/EOG i nie mogą one zostać przekazane poza to terytorium, chyba że są zgodne z art. 45, 46 lub 49 rozporządzenia (UE) 2016/679 albo z art. 47, 48 lub 50 rozporządzenia (UE) 2018/1725.

Zgodnie z art. 40 rozporządzenia (UE) 2023/988 Komisja może przekazywać państwom trzecim lub organizacjom międzynarodowym wybrane informacje ze swojego systemu wczesnego ostrzegania Safety Gate oraz otrzymywać odpowiednie informacje dotyczące bezpieczeństwa produktów oraz środków zapobiegawczych, ograniczających i naprawczych podejmowanych przez te państwa trzecie lub organizacje międzynarodowe. Wszelka wymiana informacji na podstawie art. 40 rozporządzenia (UE) 2023/988, w zakresie, w jakim dotyczy ona danych osobowych, odbywa się zgodnie z unijnymi przepisami o ochronie danych.

4.4. Odbiorcy danych osobowych

Dostępu do danych osobowych udziela się wyłącznie upoważnionym pracownikom i podwykonawcom Komisji i organów krajowych do celów zarządzania i posługiwania się systemem wczesnego ostrzegania Safety Gate. Dostęp ten musi podlegać następującym wymogom w zakresie identyfikatora i hasła:

— System wczesnego ostrzegania Safety Gate jest otwarty wyłącznie dla Komisji i użytkowników konkretnie wyznaczonych przez organy państw członkowskich UE i państw EFTA/EOG, a także organy Zjednoczonego Królestwa w odniesieniu do użytkowników z Irlandii Północnej.

— Dostęp do danych osobowych zgromadzonych w systemie wczesnego ostrzegania Safety Gate przyznaje się wyłącznie wyznaczonym i upoważnionym użytkownikom aplikacji, którzy posiadają identyfikator użytkownika/hasło. Dostęp do aplikacji i przyznanie hasła są możliwe jedynie na wniosek właściwego organu krajowego pod ogólnym nadzorem zespołu ds. Safety Gate w Komisji.

— Dostępu do zgromadzonych danych osobowych udziela się pracownikom Komisji odpowiedzialnym za prowadzenie danej operacji przetwarzania danych oraz upoważnionym osobom zgodnie z zasadą ograniczonego dostępu. Pracownicy tych służb i organów muszą przestrzegać regulaminowych, a także – w razie potrzeby – dodatkowych zobowiązań umownych do zachowania poufności.

Dostęp do zgromadzonych danych osobowych mają następujące osoby:

a) pracownicy i podwykonawcy Komisji;

b) wyznaczone punkty kontaktowe i inspektorzy z organów nadzoru rynku państw członkowskich i państw EFTA/EOG, a także organów Zjednoczonego Królestwa w odniesieniu do użytkowników z Irlandii Północnej;

c) określeni inspektorzy z organów odpowiedzialnych za kontrole granic zewnętrznych państw członkowskich UE i państw EFTA/EOG.

Osoby, które mają dostęp do wszystkich zgromadzonych danych osobowych i które mają możliwość ich modyfikowania, na wniosek, to:

a) członkowie zespołu ds. Safety Gate w Komisji;

b) pracownicy pomocy technicznej Safety Gate w Komisji.

Wykaz wszystkich punktów kontaktowych Safety Gate, zawierający ich dane kontaktowe (imię, nazwisko, nazwa organu, adres organu, numer telefonu, adres e-mail) udostępnia się na portalu Safety Gate ([3]). Zarządzanie użytkownikami na szczeblu krajowym kontrolują punkty kontaktowe Safety Gate za pośrednictwem systemu wczesnego ostrzegania Safety Gate.

([3]) https://ec.europa.eu/safety-gate/#/screen/pages/contacts.

Wszyscy użytkownicy mają dostęp do treści zgłoszeń o statusie „zatwierdzone przez KE". Jedynie krajowi użytkownicy systemu wczesnego ostrzegania Safety Gate mają dostęp do projektu swoich zgłoszeń (przed przekazaniem ich KE). Pracownicy Komisji i osoby upoważnione mają dostęp do zgłoszeń o statusie „przekazano KE".

Każdy współadministrator informuje wszystkich pozostałych współadministratorów o każdym przypadku przekazania danych osobowych odbiorcom w państwach trzecich lub organizacjach międzynarodowych.

5. OKREŚLONE OBOWIĄZKI POSZCZEGÓLNYCH WSPÓŁADMINISTRATORÓW

Komisja gwarantuje i jest odpowiedzialna za:

a) podejmowanie decyzji dotyczących sposobów, wymogów i celów przetwarzania;

b) rejestrowanie operacji przetwarzania danych;

c) ułatwienie korzystania z praw przez osoby, których dane dotyczą;

d) rozpatrywanie wniosków osób, których dane dotyczą;

e) podejmowanie decyzji dotyczących ograniczenia stosowania praw osób, których dane dotyczą, lub odstępstw od tych praw, jeśli jest to konieczne i proporcjonalne;

f) uwzględnienie ochrony prywatności już w fazie projektowania i zapewnienie domyślnej ochrony prywatności;

g) określanie i ocenę zgodności z prawem, konieczności i proporcjonalności przesyłania i przekazywania danych osobowych;

h) w razie potrzeby przeprowadzanie wcześniejszych konsultacji z Europejskim Inspektorem Ochrony Danych;

i) zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności;

j) współpracę z Europejskim Inspektorem Ochrony Danych, na jego wniosek, w zakresie wykonywania jego zadań.

Organy krajowe gwarantują i są odpowiedzialne za:

a) rejestrowanie operacji przetwarzania danych;

b) zapewnianie, aby przetwarzane dane osobowe były odpowiednie, dokładne, istotne i ograniczone do tego, co jest niezbędne do osiągnięcia celu;

c) zapewnienie osobom, których dane dotyczą, przejrzystych informacji i komunikacji o ich prawach;

d) ułatwienie korzystania z praw przez osoby, których dane dotyczą;

e) korzystanie wyłącznie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia (UE) 2016/679 i chroniło prawa osób, których dane dotyczą;

f) uregulowanie przetwarzania prowadzonego przez podmiot przetwarzający na podstawie umowy lub aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego zgodnie z art. 28 rozporządzenia (UE) 2016/679;

g) w razie potrzeby przeprowadzanie wcześniejszych konsultacji z krajowym organem nadzorczym;

h) zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności;

i) współpracę z krajowym organem nadzorczym, na jego wniosek, w zakresie wykonywania jego zadań.

6. CZAS TRWANIA PRZETWARZANIA

Współadministratorzy nie zatrzymują ani nie przetwarzają danych osobowych przez okres dłuższy niż jest to niezbędne do realizacji uzgodnionych celów i zobowiązań określonych w niniejszym rozporządzeniu, tj. przez okres konieczny do osiągnięcia celu, w którym dane te były gromadzone lub przetwarzane. W szczególności:

a) Dane kontaktowe użytkowników systemu wczesnego ostrzegania Safety Gate przechowuje się w systemie, dopóki osoby te są użytkownikami. Dane kontaktowe usuwa się z systemu wczesnego ostrzegania Safety Gate niezwłocznie po otrzymaniu informacji, że dana osoba nie jest już użytkownikiem systemu.

b) Dane kontaktowe inspektorów z organów nadzoru rynku państw członkowskich i państw EFTA/EOG, a także inspektorów z organów odpowiedzialnych za kontrole granic zewnętrznych podane w zgłoszeniach i uwagach przechowuje się w systemie przez okres pięciu lat od zatwierdzenia zgłoszenia lub uwagi.

c) Dane osobowe innych osób fizycznych, które mogły zostać ujęte w systemie, przechowuje się w formie umożliwiającej identyfikację przez 30 lat od momentu wprowadzenia informacji do systemu wczesnego ostrzegania Safety Gate, co odpowiada szacunkowej maksymalnej długości cyklu życia kategorii produktów takich jak urządzenia elektryczne lub pojazdy silnikowe.

Komisja blokuje, koryguje lub usuwa dane osób, których dane dotyczą, na ich uzasadniony wniosek w terminie jednego miesiąca od otrzymania wniosku.

7. ODPOWIEDZIALNOŚĆ ZA NIEPRZESTRZEGANIE PRZEPISÓW

Komisja ponosi odpowiedzialność za nieprzestrzeganie przepisów zgodnie z rozdziałem VIII rozporządzenia (UE) 2018/1725.

Organy państw członkowskich UE ponoszą odpowiedzialność za nieprzestrzeganie przepisów zgodnie z rozdziałem VIII rozporządzenia (UE) 2016/679.

8. WSPÓŁPRACA MIĘDZY WSPÓŁADMINISTRATORAMI

Każdy współadministrator, po otrzymaniu odnośnego wniosku, zapewnia szybką i skuteczną pomoc pozostałym współadministratorom w wykonaniu niniejszego rozporządzenia, przestrzegając przy tym wszystkich mających zastosowanie wymogów zawartych odpowiednio w rozporządzeniach (UE) 2018/1725 i (UE) 2016/679 oraz innych mających zastosowanie przepisów o ochronie danych.

9. ROZSTRZYGANIE SPORÓW

Współadministratorzy dążą do polubownego rozstrzygania wszelkich sporów wynikających z wykładni lub stosowania niniejszego rozporządzenia lub z nim związanych.

Jeśli w dowolnym momencie między współadministratorami wystąpi wątpliwość, spór lub różnica w odniesieniu do niniejszej rozporządzenia lub w związku z nim, współadministratorzy dokładają wszelkich starań, aby rozstrzygnięcie nastąpiło w drodze konsultacji.

Zaleca się, aby wszystkie spory rozstrzygano na szczeblu operacyjnym w miarę ich powstawania oraz aby ich rozstrzyganiem zajmowały się punkty kontaktowe, o których mowa w pkt 10 niniejszego załącznika i które są podane na portalu Safety Gate.

Celem konsultacji jest rozpatrzenie i uzgodnienie, w miarę możliwości, działań podejmowanych w celu rozwiązania problemu. W tym celu współadministratorzy negocjują ze sobą w dobrej wierze. Każdy współadministrator musi odpowiedzieć na wniosek o polubowne rozstrzygnięcie sporu w ciągu siedmiu dni roboczych od otrzymania takiego wniosku. Termin polubownego rozstrzygnięcia sporu wynosi 30 dni roboczych od daty otrzymania wniosku.

Jeśli sporu nie można rozstrzygnąć polubownie, każdy współadministrator może skorzystać z mediacji lub postępowania sądowego w następujący sposób:

a) w przypadku mediacji współadministratorzy wspólnie wyznaczają akceptowanego przez każdego z nich mediatora, który będzie odpowiedzialny za ułatwienie rozstrzygnięcia sporu w terminie dwóch miesięcy od skierowania do niego sporu;

b) w przypadku postępowania sądowego sprawę kieruje się do Trybunału Sprawiedliwości Unii Europejskiej zgodnie z art. 272 Traktatu o funkcjonowaniu Unii Europejskiej.

10. PUNKTY KONTAKTOWE DO SPRAW WSPÓŁPRACY MIĘDZY WSPÓŁADMINISTRATORAMI

Każdy współadministrator wyznacza jeden punkt kontaktowy, z którym pozostali współadministratorzy mogą się kontaktować w sprawie zapytań, skarg oraz informacji w zakresie niniejszego rozporządzenia.

Szczegółowy wykaz wszystkich punktów kontaktowych wyznaczonych przez Komisję i organy krajowe, zawierający ich dane kontaktowe (imię, nazwisko, nazwa organu, adres organu, numer telefonu, faksu, adres e-mail) udostępnia się na portalu Ascety Gate.