# DECYZJE

## DECYZJA WYKONAWCZA KOMISJI (UE) 2023/975

**z dnia 15 maja 2023 r.**

**zmieniająca decyzję wykonawczą Komisji (UE) 2019/417 ustanawiającą wytyczne dotyczące zarządzania unijnym systemem szybkiej informacji „RAPEX" utworzonym na mocy art. 12 dyrektywy 2001/95/WE Parlamentu Europejskiego i Rady w sprawie ogólnego bezpieczeństwa produktów oraz funkcjonującym w jego ramach systemem zgłoszeń**

*(notyfikowana jako dokument nr C(2023) 2817)*

**(Tekst mający znaczenie dla EOG)**

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów ([1]), w szczególności jej art. 11 ust. 1 akapit trzeci i pkt 8 załącznika II do tej dyrektywy,

uwzględniając 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 ([2]), w szczególności jego art. 20,

uwzględniając 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 ([3]), w szczególności jego art. 28 ust. 1,

uwzględniając 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 ([4]), w szczególności jego art. 26 ust. 1,

po konsultacji z komitetem powołanym na mocy art. 15 ust. 1 dyrektywy 2001/95/WE,

po konsultacji z Europejskim Inspektorem Ochrony Danych zgodnie z art. 42 rozporządzenia (UE) 2018/1725,

a także mając na uwadze, co następuje:

(1) Decyzja wykonawcza Komisji (UE) 2019/417 ([5]) określa wytyczne dotyczące zarządzania unijnym systemem szybkiej informacji „RAPEX" utworzonym na mocy art. 12 dyrektywy 2001/95/WE oraz funkcjonującym w jego ramach systemem zgłoszeń.

([1]) Dz.U. L 11 z 15.1.2002, s. 4.
([2]) Dz.U. L 169 z 25.6.2019, s. 1.
([3]) Dz.U. L 295 z 21.11.2018, s. 39.
([4]) Dz.U. L 119 z 4.5.2016, s. 1.
([5]) 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).

(2) Art. 28 rozporządzenia (UE) 2018/1725 stanowi, że jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. Obowiązki poszczególnych współadministratorów mogą zostać określone w prawie Unii, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 15 i 16 rozporządzenia (UE) 2018/1725.

(3) Art. 26 rozporządzenia (UE) 2016/679 stanowi, że jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych osobowych, uznaje się ich za współadministratorów. Obowiązki poszczególnych współadministratorów mogą zostać określone w prawie Unii, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 rozporządzenia (UE) 2016/679.

(4) Komisja i organy krajowe pełnią funkcję współadministratorów przetwarzania danych w systemie Safety Gate/RAPEX.

(5) Należy określić podział ról i obowiązków oraz ustalenia między Komisją a organami krajowymi działającymi jako współadministratorzy na mocy art. 28 rozporządzenia (UE) 2018/1725 i art. 26 rozporządzenia (UE) 2016/679.

(6) Należy zatem odpowiednio zmienić decyzję wykonawczą (UE) 2019/417,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

*Artykuł 1*

W decyzji wykonawczej (UE) 2019/417 wprowadza się następujące zmiany:

1) art. 1 otrzymuje brzmienie:

„*Artykuł 1*

1. W załączniku I do niniejszej decyzji zawarto wytyczne dotyczące zarządzania unijnym systemem szybkiej informacji »RAPEX« utworzonym na mocy art. 12 dyrektywy 2001/95/WE oraz funkcjonującym w jego ramach systemem zgłoszeń.

2. W załączniku II do niniejszej decyzji określono zasady współadministrowania unijnym systemem szybkiej informacji »RAPEX«.";

2) załącznik otrzymuje nazwę „Załącznik I";

3) dodaje się załącznik II w brzmieniu określonym w załączniku do niniejszej decyzji.

*Artykuł 2*

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 15 maja 2023 r.

*W imieniu Komisji*
Didier REYNDERS
*Członek Komisji*

*ZAŁĄCZNIK*

*„ZAŁĄCZNIK II*

**WSPÓŁADMINISTROWANIE UNIJNYM SYSTEMEM SZYBKIEJ INFORMACJI »RAPEX« UTWORZONYM NA MOCY ART. 12 DYREKTYWY 2001/95/WE PARLAMENTU EUROPEJSKIEGO I RADY [1] (DYREKTYWA W SPRAWIE OGÓLNEGO BEZPIECZEŃSTWA PRODUKTÓW)**

1. ***Przedmiot i opis przetwarzania***

Aplikacja Safety Gate/RAPEX jest systemem powiadamiania służącym 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. Celem tego systemu powiadamiania jest:

— uniemożliwienie dostarczania konsumentom niebezpiecznych produktów na rynku wewnętrznym,

— w razie potrzeby, podjęcie środków naprawczych, takich jak wycofanie takich produktów z obrotu lub odzyskanie ich od użytkowników.

Wymiana informacji dotyczy środków i działań zapobiegawczych i restrykcyjnych podejmowanych w odniesieniu do niebezpiecznych produktów konsumenckich i specjalistycznych, z wyjątkiem żywności, pasz, produktów farmaceutycznych i wyrobów medycznych. System Safety Gate/RAPEX obejmuje zarówno środki zastosowane przez organy krajowe, jak i środki podjęte dobrowolnie przez podmioty gospodarcze.

2. ***Zakres współadministrowania***

Komisja i organy krajowe działają jako współadministratorzy przetwarzania danych w systemie Safety Gate/RAPEX. »Organy krajowe« to wszystkie organy państw członkowskich i organy państw EFTA/EOG, które działają w obszarze bezpieczeństwa produktów konsumenckich i należą do sieci Safety Gate/RAPEX, łącznie z organami nadzoru rynku odpowiedzialnymi za monitorowanie zgodności produktów z wymogami bezpieczeństwa i organami odpowiedzialnymi za kontrole granic zewnętrznych.

Do celów art. 26 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 [2] i art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 [3] Komisja jako współadministrator danych osobowych jest odpowiedzialna za następujące czynności przetwarzania:

1) Komisja może przetwarzać informacje dotyczące środków wprowadzonych względem produktów stwarzających poważne zagrożenie, przywożonych do Unii i Europejskiej i Europejskiego Obszaru Gospodarczego lub z nich wywożonych, w celu przekazania tych informacji punktom kontaktowym RAPEX.

2) Komisja może przetwarzać informacje otrzymane od państw trzecich, organizacji międzynarodowych, przedsiębiorstw lub innych systemów wczesnego ostrzegania, dotyczące produktów stwarzających zagrożenie, pochodzących z UE i spoza UE, w celu przekazania tych informacji organom krajowym.

Komisja odpowiada za zapewnienie przestrzegania obowiązków i warunków określonych w rozporządzeniu (UE) 2018/1725 w odniesieniu do tych działań.

---

[1] 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).

[2] 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).

[3] 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).

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

1) Organy krajowe mogą przetwarzać informacje zgodnie z art. 11 i 12 dyrektywy 2001/95/WE oraz art. 20 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 ([4]) w celu przekazania tych informacji Komisji i innym państwom członkowskim oraz państwom EFTA/EOG.

2) Organy krajowe mogą przetwarzać informacje wynikające z ich działań następczych przeprowadzonych w związku ze zgłoszeniami w systemie Safety Gate/RAPEX w celu przekazania tych informacji Komisji i innym państwom członkowskim oraz państwom EFTA/EOG.

Organy krajowe odpowiadają za zapewnienie przestrzegania obowiązków i warunków określonych w rozporządzeniu (UE) 2016/679 w odniesieniu do tych działań.

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 Safety Gate/RAPEX

Następujące dane mogą być przetwarzane:

— imię,

— nazwisko,

— adres e-mail,

— kraj,

— preferowany język.

b) Dane kontaktowe autorów i osób zatwierdzających zgłoszenia i uwagi przekazane za pośrednictwem systemu Safety Gate/RAPEX.

Do autorów i osób zatwierdzających należą:

— krajowe punkty kontaktowe systemu Safety Gate/RAPEX 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, tacy jak urzędnicy, pracownicy zatrudnieni na czas określony, pracownicy kontraktowi, stażyści i usługodawcy zewnętrzni.

Następujące dane mogą być przetwarzane:

— imiona autorów i osób zatwierdzających zgłoszenia i uwagi przekazane za pośrednictwem systemu Safety Gate/RAPEX,

— nazwiska autorów i osób zatwierdzających zgłoszenia i uwagi przekazane za pośrednictwem systemu Safety Gate/RAPEX,

— nazwy organów będących autorem lub podmiotem zatwierdzającym zgłoszenia i uwagi przekazane za pośrednictwem systemu Safety Gate/RAPEX,

— adresy organów będących autorem lub podmiotem zatwierdzającym zgłoszenia i uwagi przekazane za pośrednictwem systemu Safety Gate/RAPEX,

([4]) 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).

— adresy e-mail autorów i osób zatwierdzających zgłoszenia i uwagi przekazane za pośrednictwem systemu Safety Gate/RAPEX,

— numery telefonów autorów i osób zatwierdzających zgłoszenia i uwagi przekazane za pośrednictwem systemu Safety Gate/RAPEX.

c) Ponadto w systemie mogą dodatkowo zostać ujęte dwa rodzaje danych osobowych:

(i) Kiedy konieczne jest wykrycie produktów niebezpiecznych zdefiniowanych w art. 2 lit. c) dyrektywy 2001/95/WE, dane kontaktowe podmiotów gospodarczych (producentów, eksporterów, importerów, dystrybutorów lub sprzedawców detalicznych) mogą zawierać dane osobowe, które zostaną ujęte w systemie. Takie dane są wprowadzane do systemu Safety Gate/RAPEX wyłącznie przez organy krajowe na podstawie informacji zgromadzonych podczas dochodzenia.

Następujące dane podmiotów gospodarczych mogą być przetwarzane:

— nazwa,

— adres,

— miejscowość,

— kraj,

— dane kontaktowe: 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 i które zostały dodatkowo ujęte w innych dokumentach, np. w sprawozdaniach z badań. Te dane osobowe znajdują się w załącznikach i nie można ich wyszukiwać. Państwa członkowskie są proszone o usunięcie takich danych przed przedłożeniem sprawozdania, jeżeli nie uważają tych danych za niezbędne do celów systemu.

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 Safety Gate/RAPEX,

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

Użytkownicy systemu Safety Gate/RAPEX są informowani o przysługujących im prawach za pośrednictwem oświadczenia o ochronie prywatności dostępnego w systemie Safety Gate/RAPEX.

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 i/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 odpowiednio z rozporządzenia (UE) 2018/1725 i rozporządzenia (UE) 2016/679 w odniesieniu do każdego ze współadministratorów i przeciwko każdemu z nich.

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 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 odpowiednim 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 ([5]) 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;

([5]) 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).

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 wszelkie cyberincydenty, w tym naruszenia ochrony danych osobowych, do których dochodzi w wyniku naruszenia zobowiązań danego współadministratora wynikających z niniejszej decyzji 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 pozostałych współadministratorów.

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 pozostałych współadministratorów.

### 4.3. **Lokalizacja danych osobowych**

Dane osobowe gromadzone do celów procesu powiadamiania za pośrednictwem systemu Safety Gate/RAPEX przechowuje i gromadzi się w aplikacji Safety Gate/RAPEX obsługiwanej przez Komisję 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 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. 12 ust. 4 dyrektywy 2001/95/WE dostęp do systemu Safety Gate/RAPEX przysługuje państwom ubiegającym się o członkostwo, państwom trzecim lub organizacjom międzynarodowym w ramach umowy między UE a tymi państwami lub organizacjami międzynarodowymi stosownie do warunków określonych w tych umowach. Można przekazywać wybrane informacje z systemu Safety Gate/RAPEX. Takie informacje nie mogą zawierać danych osobowych.

### 4.4. **Odbiorcy**

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

— System Safety Gate/RAPEX 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 zgromadzonych danych osobowych w systemie Safety Gate/RAPEX 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/RAPEX 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/RAPEX w Komisji;

b) pracownicy pomocy technicznej Safety Gate/RAPEX w Komisji.

Wykaz wszystkich punktów kontaktowych Safety Gate/RAPEX (użytkowników wyznaczonych przez organy krajowe w państwach UE/EOG) zawierający ich dane kontaktowe (imię, nazwisko, nazwa organu, adres organu, numer telefonu, faksu, adres e-mail) udostępnia się publicznie na stronie internetowej Safety Gate w portalu Europa ([6]). Zarządzanie użytkownikami na szczeblu krajowym kontrolują krajowe punkty kontaktowe Safety Gate/RAPEX za pośrednictwem aplikacji Safety Gate/RAPEX.

Wszyscy użytkownicy mają dostęp do treści zgłoszeń o statusie „EC validated" (zatwierdzone przez KE). Jedynie krajowi użytkownicy Safety Gate/RAPEX 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 wszelkich przypadkach przekazywania 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 tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

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

([6]) https://ec.europa.eu/safety/consumers/consumers_safety_gate/menu/documents/Safety_Gate_contacts.pdf

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, 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 tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

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 niniejszej decyzji, tj. przez okres konieczny do osiągnięcia celu, w którym dane te były gromadzone lub przetwarzane. W szczególności:

a) Dane kontaktowe użytkowników aplikacji Safety Gate/RAPEX przechowuje się w systemie, dopóki osoby te są użytkownikami. Dane kontaktowe usuwa się z aplikacji 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 Safety Gate/RAPEX, 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 niniejszej decyzji, przestrzegając przy tym wszystkich mających zastosowanie wymogów zawartych odpowiednio w rozporządzeniu (UE) 2018/1725 i rozporządzeniu (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 niniejszej decyzji lub z nią związanych.

Jeśli w dowolnym momencie między współadministratorami wystąpi wątpliwość, spór lub różnica w odniesieniu do niniejszej decyzji lub w związku z niniejszą decyzją, współadministratorzy dołożą 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 ogólnodostępnej stronie internetowej Safety Gate w portalu Europa.

Celem konsultacji jest dokonanie przeglądu i uzgodnienie, w miarę możliwości, działań podejmowanych w celu rozwiązania powstałego problemu, a współadministratorzy prowadzą w tym celu negocjacje w dobrej wierze. Każdy współadministrator musi odpowiedzieć na wniosek o polubowne rozstrzygnięcie sporu w ciągu 7 dni roboczych od złożenia takiego wniosku. Termin polubownego rozstrzygnięcia sporu wynosi 30 dni roboczych od daty złożenia 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 niniejszej decyzji.

Szczegółowy wykaz wszystkich punktów kontaktowych wyznaczonych przez Komisję i organy krajowe w państwach UE/EOG, zawierający ich dane kontaktowe (imię, nazwisko, nazwa organu, adres organu, numer telefonu, faksu, adres e-mail) udostępnia się publicznie na stronie internetowej Safety Gate w portalu Europa.”.