

Zalecenie



**Zalecenie 01/2019 w sprawie projektu wykazu
sporządzonego przez Europejskiego Inspektora Ochrony
Danych dotyczącego rodzajów operacji przetwarzania
podlegających wymogowi dokonania oceny skutków dla
ochrony danych (art. 39 ust. 4 rozporządzenia (UE)
2018/1725)**

Przyjęte 10 lipca 2019 r.

Spis treści

1	STRESZCZENIE STANU FAKTYCZNEGO.....	4
2	OCENA.....	4
2.1	Ogólne uzasadnienie EROD dotyczące przedłożonego wykazu.....	4
2.2	Analiza projektu wykazu	5
3	WNIOSEK.....	8

Europejska Rada Ochrony Danych (EROD)

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady 2016/679/UE 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 (zwanego dalej „RODO”),

uwzględniając art. 39 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725/UE 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 (zwanego dalej „rozporządzeniem 2018/1725”),

uwzględniając art. 12 i 22 swojego regulaminu z dnia 25 maja 2018 r., ze zmianami z dnia 23 listopada 2018 r.,

a także mając na uwadze, co następuje:

(1) Głównym zadaniem EROD jest zapewnienie spójnego stosowania rozporządzenia 2016/679 (zwanego dalej „RODO”) na całym terytorium Europejskiego Obszaru Gospodarczego. Zgodnie z art. 70 ust. 1 lit. e) RODO Europejska Rada Ochrony Danych bada w tym celu na wniosek jednego z jej członków wszelkie kwestie dotyczące stosowania tego rozporządzenia i wydaje wytyczne, zalecenia oraz określa najlepsze praktyki, aby zachęcić do jego spójnego stosowania. Art. 39 ust. 6 rozporządzenia 2018/1725 stanowi, że przed przyjęciem projektu wykazu Europejski Inspektor Ochrony Danych zwraca się do EROD o zbadanie – zgodnie z art. 70 ust. 1 lit. e) RODO – takiego projektu wykazu operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych zgodnie z art. 39 ust. 4 rozporządzenia 2018/1725. Obowiązek ten ma zastosowanie w zakresie, w jakim wykaz ten odnosi się do operacji przetwarzania prowadzonych przez administratora danych w rozumieniu art. 3 pkt 8 rozporządzenia 2018/1725, działającego wspólnie z co najmniej jednym administratorem innym niż instytucje i organy Unii. Celem niniejszego zalecenia jest zatem zapewnienie spójności z podejściem przyjętym uprzednio w odniesieniu do projektów wykazów organów nadzorczych (zwanych dalej „organami nadzorczymi”). EROD dążyła do osiągnięcia spójności, po pierwsze – zwracając się do organów nadzorczych o uwzględnienie niektórych rodzajów przetwarzania w swoich wykazach, po drugie – zwracając się do nich o usunięcie pewnych kryteriów, które zdaniem EROD niekoniecznie stwarzają wysokie ryzyko dla osób, których dane dotyczą, i po trzecie – wzywając te organy do stosowania określonych kryteriów w sposób zharmonizowany.

(4) Zgodnie z art. 39 ust. 1 rozporządzenia 2018/1725 dokonanie oceny skutków dla ochrony danych jest dla administratora obowiązkowe wyłącznie w przypadku, gdy przetwarzanie danych „z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”. W art. 39 ust. 3 rozporządzenia 2018/1725 wymieniono, w jakim przypadku istnieje prawdopodobieństwo wystąpienia wysokiego ryzyka. Jest to niewyczerpujący wykaz, który odpowiada brzmieniu art. 35 ust. 3 RODO. W wytycznych dotyczących oceny skutków dla ochrony danych¹,

¹ Grupa Robocza Art. 29, Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679 (WP 248 rev. 01).

zatwierdzonych przez Europejską Radę Ochrony Danych², Grupa Robocza Art. 29 wyjaśniła kryteria, które mogą pomóc w ustaleniu, w jakich przypadkach operacje przetwarzania podlegają wymogowi dokonania oceny skutków dla ochrony danych. W wytycznych Grupy Roboczej Art. 29 nr WP 248 stwierdzono, że w większości przypadków administrator danych może uznać, że dokonania oceny skutków dla ochrony danych wymaga przetwarzanie danych spełniające dwa kryteria. W niektórych przypadkach administrator może jednak uznać, że dokonania tej oceny wymaga przetwarzanie spełniające tylko jedno z tych kryteriów.

(5) Wykazy opracowane przez Europejskiego Inspektora Ochrony Danych mają ten sam cel – określenie operacji przetwarzania, które z dużym prawdopodobieństwem mogą powodować wysokie ryzyko, i operacji przetwarzania, które w związku z tym wymagają dokonania oceny skutków dla ochrony danych. Kryteria opracowane w wytycznych Grupy Roboczej Art. 29 mają zasadniczo zastosowanie.

PRZYJMUJE NINIEJSZE ZALECENIE:

1 STRESZCZENIE STANU FAKTYCZNEGO

1. Zgodnie z art. 39 ust. 4 rozporządzenia 2018/1725 Europejski Inspektor Ochrony Danych przedstawił EROD swój projekt wykazu 18 marca 2019 r., a następnie jego zmienioną wersję 21 czerwca 2019 r.
2. Dokument przedłożony przez Europejskiego Inspektora Ochrony Danych zawierał również część dotyczącą art. 39 ust. 5 rozporządzenia 2018/1725. Zmieniony projekt dokumentu wyraźnie wskazuje, że zawarty w nim wykaz na podstawie art. 39 ust. 5 ma zastosowanie wyłącznie w przypadkach, w których instytucje lub organy Unii są współadministratorami lub jedynymi administratorami. W szczególności projekt wykazu na podstawie art. 39 ust. 5 obejmuje operacje przetwarzania dotyczące przetwarzania danych przez instytucje lub organy Unii do celów ich wewnętrznego zarządzania, prowadzone bez udziału administratorów innych niż instytucje i organy Unii.
3. W związku z tym EROD zwraca uwagę, że ta druga część dokumentu nie wchodzi w zakres stosowania art. 39 ust. 6 rozporządzenia 2018/1725. Przepis ten określa, że obowiązek zwrócenia się do EROD o wydanie zalecenia ma zastosowanie wyłącznie do tych pozycji, które dotyczą operacji przetwarzania, w przypadku których administrator danych podlegający przepisom rozporządzenia 2018/1725 działa wspólnie z co najmniej jednym administratorem innym niż instytucje lub organy Unii. W związku z tym EROD nie będzie komentowała tej części projektu dokumentu.

2 OCENA

2.1 Ogólne uzasadnienie EROD dotyczące przedłożonego wykazu

4. Wykaz przedłożony EROD analizuje się jako szczegółowe rozwinięcie art. 39 ust. 1 rozporządzenia 2018/1725, który to przepis zawsze będzie miał znaczenie rozstrzygające. W związku z tym wspomnianego wykazu nie należy traktować jako wykazu wyczerpującego.

² EROD, zatwierdzenie 1/2018.

5. EROD zwraca uwagę na art. 39 ust. 10 rozporządzenia 2018/1725, zgodnie z którym nie wymaga się dokonania oceny skutków dla ochrony danych, jeśli dana operacja przetwarzania lub dany zestaw operacji ma podstawę prawną w akcie prawnym przyjętym na podstawie Traktatów, a ocena skutków dla ochrony danych została już przeprowadzona w ramach ogólnej oceny skutków poprzedzającej przyjęcie tego aktu prawnego. W takim przypadku nie ma zastosowania art. 39 ust. 1–6, chyba że dany akt prawny stanowi inaczej.
6. Niniejsze zalecenie zasadniczo nie obejmuje pozycji przedstawionych przez Europejskiego Inspektora Ochrony Danych, które uznano za niewchodzące w zakres art. 39 ust. 6 rozporządzenia 2018/1725. Dotyczy to pozycji, które nie odnoszą się do operacji przetwarzania, w przypadku których administrator działa wspólnie z co najmniej jednym administratorem innym niż instytucje lub organy Unii. Ponieważ jednak Europejski Inspektor Ochrony Danych podjął decyzję o przyjęciu jednego wykazu w odniesieniu do obu tych rodzajów operacji przetwarzania, niniejsze zalecenie stosuje się de facto do obu tych kategorii operacji przetwarzania.
7. Zalecenie ma na celu dostosowanie do podstawowego zestawu operacji przetwarzania, o których umieszczenie w swoich wykazach EROD zwróciła się do wszystkich organów nadzorczych, o ile operacje te nie zostały jeszcze umieszczone w tych wykazach.
8. Oznacza to, że w odniesieniu do ograniczonej liczby rodzajów operacji przetwarzania, które zostaną zdefiniowane w sposób zharmonizowany, EROD zaleca Europejskiemu Inspektorowi Ochrony Danych wprowadzenie wymogu dokonania oceny skutków dla ochrony danych.
9. Jeśli w niniejszym zaleceniu nie ma mowy o określonych pozycjach zawartych w przedłożonym wykazie dotyczącym oceny skutków dla ochrony danych, oznacza to, że EROD nie zwraca się do Europejskiego Inspektora Ochrony Danych o podjęcie dalszych działań.
10. EROD przypomina ponadto, że kluczowe znaczenie dla administratorów danych i podmiotów przetwarzających dane ma przejrzystość. Aby doprecyzować pozycje w wykazie, EROD zaleca zawarcie w wykazach wyraźnych odniesień, w przypadku każdego rodzaju przetwarzania, do kryteriów określonych w wytycznych w celu zwiększenia przejrzystości.

2.2 Analiza projektu wykazu

11. Biorąc pod uwagę, że:
 - a) art. 39 ust. 1 rozporządzenia 2018/1725 wymaga dokonania oceny skutków dla ochrony danych, jeżeli działalność związana z przetwarzaniem może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych; oraz
 - b) art. 39 ust. 3 rozporządzenia 2018/1725 zawiera niewyczerpujący wykaz rodzajów przetwarzania, które wymagają oceny skutków dla ochrony danych;

EROD wydaje następujące zalecenia:

DANE WRAŻLIWE

12. W projekcie wykazu wymienia się „dane wrażliwe” jako następujące kryterium: „Dane wrażliwe: dane ujawniające pochodzenie etniczne lub rasowe, poglądy polityczne, przekonania religijne lub światopoglądowe, lub przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące stanu zdrowia, seksualności

lub orientacji seksualnej, wyroków skazujących i naruszeń prawa lub związanych z nimi środków bezpieczeństwa lub dane w inny sposób uznane za wrażliwe”.

13. Mimo że brzmienie jest bardzo podobne do wytycznych (WP 248 rev. 01) dotyczących oceny skutków dla ochrony danych opracowanych przez Grupę Roboczą Art. 29 i zatwierdzonych przez EROD, istnieje pewna istotna różnica. O ile w projekcie wykazu użyto sformułowania „lub dane w inny sposób uznane za wrażliwe”, w wytycznych mowa jest o „danych o bardzo osobistym charakterze”.
14. EROD zwraca uwagę, że w RODO terminu „dane wrażliwe” nie użyto w żadnym z artykułów, chociaż użyto go w dwóch motywach, przy czym należy go interpretować wyłącznie w odniesieniu do kategorii danych wymienionych w art. 9 i 10 RODO. Aby uniknąć niejasności, EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę sformułowania „lub dane w inny sposób uznane za wrażliwe” i użycie dokładnie tego samego sformułowania, które występuje w wytycznych dotyczących oceny skutków dla ochrony danych.

PRZETWARZANIE NA DUŻĄ SKALĘ

15. EROD zwraca uwagę, że Europejski Inspektor Ochrony Danych odwołuje się do wewnętrznej telefonicznej bazy danych należącej do instytucji UE jako negatywnego przykładu przetwarzania na dużą skalę. Niezależnie od tego, czy rzeczywiście wymagana jest ocena skutków dla ochrony danych, nie jest jasne, dlaczego telefoniczna baza danych instytucji UE sama w sobie nie wchodzi w zakres pojęcia przetwarzania na dużą skalę, zwłaszcza że może ona potencjalnie zawierać dane osobowe dużej liczby osób. EROD przypomina również, że pojęcie „na dużą skalę” odnosi się również do odsetka danej populacji, jak określono w wytycznych dotyczących inspektorów ochrony danych, przyjętych w grudniu 2016 r., zmienionych w dniu 5 kwietnia 2017 r. i zatwierdzonych przez EROD. EROD zaleca użycie innego przykładu.

ZBIORY DANYCH ZESTAWIANE LUB ŁĄCZONE Z RÓŻNYCH OPERACJI PRZETWARZANIA DANYCH

16. EROD zwraca uwagę, że przykład wykorzystany do zobrazowania operacji przetwarzania, w których występują zbiory danych zestawiane lub łączone z różnych operacji przetwarzania danych, może budzić wątpliwości co do jego zgodności z prawem na mocy rozporządzenia 2018/1725, biorąc pod uwagę sposób, w jaki został on przedstawiony. Chociaż EROD nie jest w stanie ocenić tej zgodności z prawem i nie ma do tego kompetencji, zaleca – w celu zapewnienia jasności – podanie innego przykładu.

OSOBY, KTÓRYCH DANE DOTYCZĄ, WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY

17. EROD zwraca uwagę, że Europejski Inspektor Ochrony Danych w swojej decyzji jako przykład negatywny podaje pracowników instytucji UE w odniesieniu do standardowych procedur określonych w regulaminie pracowniczym. EROD przypomina, że w zatwierdzonych przez nią wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych (WP 248 rev. 01) pracownicy są wymienieni jako osoby, których dane dotyczą, wymagające szczególnej ochrony. Chociaż można twierdzić, że brak równowagi sił między pracodawcą a pracownikiem jest mniej rażący w kontekście „standardowych procedur” w ramach odnośnego regulaminu pracowniczego, nie można uznać, że zawsze ma to miejsce, zwłaszcza gdy pracownicy nie mają znaczącego wpływu na treść tego regulaminu. Ponadto nie jest jasne, które procedury można uznać za niestandardowe, w którym to przypadku może być potencjalnie konieczne dokonanie oceny skutków dla ochrony danych, co może

prowadzić do znacznej niejasności. W związku z tym EROD zaleca, by Europejski Inspektor Ochrony Danych zastąpił podany przykład innym.

3 WNIOSEK

18. Rada zwraca się do Europejskiego Inspektora Ochrony Danych o dokonanie następujących zmian w jego wykazie:
- jeśli chodzi o dane wrażliwe: EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę jego wykazu poprzez zmianę sformułowania „lub dane w inny sposób uznane za wrażliwe” oraz zastosowanie dokładnie takiego samego brzmienia jak w wytycznych dotyczących oceny skutków dla ochrony danych;
 - jeśli chodzi o dane przetwarzane na dużą skalę: EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę wykazu poprzez wykorzystanie innego przykładu negatywnego;
 - jeśli chodzi o zbiory danych zestawiane lub łączone z różnych operacji przetwarzania danych: EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę wykazu poprzez wykorzystanie innego przykładu;
 - jeśli chodzi o osoby, których dane dotyczą, wymagające szczególnej ochrony: EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę wykazu poprzez wykorzystanie innego przykładu negatywnego.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)