Opinia Rady (art. 64)

Opinia 19/2024 w sprawie kryteriów certyfikacji EuroPriSe dotycząca ich zatwierdzenia przez EROD jako europejskiego znaku jakości ochrony danych zgodnie z art. 42 ust. 5 (RODO)

Przyjęta 16 lipca 2024 r.

Spis treści

1. STRESZCZENIE FAKTÓW 4
2. OCENA 5
2.1 Zakres mechanizmu certyfikacji i przedmiot oceny 5
2.2 Operacje przetwarzania 5
2.3 Zgodność z prawem i zasady przetwarzania danych 6
2.4 Ogólne obowiązki administratorów danych i podmiotów przetwarzających 6
2.5 Prawa osób, których dane dotyczą 6
2.6 Zagrożenia dla praw i wolności 6
2.7 Środki techniczne i organizacyjne gwarantujące ochronę 7
2.8 Kryteria mające na celu wykazanie istnienia odpowiednich zabezpieczeń na potrzeby przekazywania danych osobowych 7
3. DODATKOWE KRYTERIA DOTYCZĄCE EUROPEJSKIEGO ZNAKU JAKOŚCI OCHRONY DANYCH 7
WNIOSKI/ZALECENIA 7
UWAGI KOŃCOWE 7

Europejska Rada Ochrony Danych,

uwzględniając art. 63, art. 64 ust. 2 lit. i art. 42 rozporządzenia 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 (dalej „RODO"),

uwzględniając Porozumienie o Europejskim Obszarze Gospodarczym (dalej „EOG"), a w szczególności jego załącznik XI i protokół 37, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 10 i 22 swojego regulaminu wewnętrznego,

(1) Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych (dalej „EROD") oraz Komisja Europejska zachęcają – w szczególności na poziomie Unii – do ustanowienia mechanizmów certyfikacji ochrony danych (dalej „mechanizmy certyfikacji") oraz znaków jakości i oznaczeń w dziedzinie ochrony danych w celu wykazania zgodności operacji przetwarzania – dokonywanych przez administratorów i podmioty przetwarzające – z RODO, z uwzględnieniem szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw[2]. Ponadto ustanowienie mechanizmów certyfikacji może zwiększyć przejrzystość i pozwolić osobom, których dane dotyczą, ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi[3].

(2) Kryteria certyfikacji stanowią integralną część mechanizmu certyfikacji. Dlatego też RODO wymaga zatwierdzenia kryteriów krajowego mechanizmu certyfikacji przez właściwy organ nadzorczy (art. 42 ust. 5 i art. 43 ust. 2 lit. b) RODO) lub, w przypadku europejskiego znaku jakości ochrony danych, przez EROD (art. 42 ust. 5 i art. 70 ust. 1 lit. o) RODO).

(3) W przypadku gdy organ nadzorczy (dalej „ON") zamierza zaproponować zatwierdzenie przez EROD europejskiego znaku jakości ochrony danych zgodnie z art. 42 ust. 5 RODO, organ nadzorczy powinien wskazać, że właściciel systemu zamierza zaoferować mechanizm certyfikacji we wszystkich państwach członkowskich. W tym przypadku główną rolą EROD jest zapewnienie spójnego stosowania RODO za pomocą mechanizmu spójności, o którym mowa w art. 63, 64 i 65 RODO. W tym kontekście, zgodnie z art. 64 ust. 2 RODO, EROD zatwierdza kryteria certyfikacji.

(4) Celem niniejszej opinii jest zapewnienie spójnego stosowania RODO, mi.in. przez organy nadzorcze, administratorów i podmioty przetwarzające w świetle podstawowych elementów, które to elementy należy opracować w mechanizmach certyfikacji. Ocenę EROD przeprowadza się przede wszystkim na podstawie „Wytycznych 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia" (dalej „wytyczne") oraz ich uzupełnienia zawierającego „Wytyczne w sprawie oceny kryteriów certyfikacji" (dalej „uzupełnienie"), dla których okres konsultacji publicznych upłynął 26 maja 2021 r.

[1] Odniesienia do „państw członkowskich" w niniejszej opinii należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Artykuł 42 ust. 1 RODO.
[3] Motyw 100 RODO.

(5) W związku z tym EROD uznaje, że każdy mechanizm certyfikacji należy rozpatrywać indywidualnie i nie ma to wpływu na ocenę jakiegokolwiek innego mechanizmu certyfikacji.

(6) Mechanizmy certyfikacji powinny umożliwić administratorom i podmiotom przetwarzającym wykazanie zgodności z RODO. Dlatego też ich kryteria powinny prawidłowo odzwierciedlać wymogi i zasady dotyczące ochrony danych osobowych określone w RODO oraz przyczyniać się do ich spójnego stosowania.

(7) Jednocześnie właściciel systemu powinien zapewniać dostosowanie mechanizmu certyfikacji do wszelkich uwzględnionych lub wykorzystanych norm ISO i praktyk certyfikacyjnych oraz zgodność tego mechanizmu z nimi.

(8) W związku z tym certyfikacje powinny stanowić wartość dodaną dla administratorów i podmiotów przetwarzających, wspomagając wdrażanie ustandaryzowanych i sprecyzowanych środków organizacyjnych i technicznych, które w sposób oczywisty ułatwiają zachowanie zgodności operacji przetwarzania z RODO i zwiększają tę zgodność, z uwzględnieniem wymogów sektorowych.

(9) EROD z zadowoleniem przyjmuje wysiłki podejmowane przez właścicieli systemów na rzecz opracowania mechanizmów certyfikacji, które są praktycznymi i potencjalnie opłacalnymi narzędziami zapewniającymi większą spójność z RODO oraz wspierają prawo do prywatności i ochrony danych osób, których dane dotyczą, poprzez zwiększenie przejrzystości.

(10) EROD przypomina, że certyfikacje są dobrowolnymi narzędziami odpowiedzialności, a stosowanie się do mechanizmu certyfikacji nie zmniejsza rozliczalności administratorów lub podmiotów przetwarzających za zgodność z RODO ani nie uniemożliwia organom nadzorczym wykonywania ich zadań i uprawnień na mocy RODO oraz odpowiednich przepisów krajowych.

(11) W niniejszej opinii EROD zajmuje się takimi kwestiami, jak zakres kryteriów oraz możliwość ich zastosowania i znaczenie we wszystkich państwach członkowskich.

(12) Niniejsza opinia poświęcona jest kryteriom certyfikacji. Jeśli EROD wymaga ogólnych informacji na temat metod oceny, aby móc dokładnie ocenić możliwość kontroli kryteriów w kontekście swojej opinii na ich temat, nie wiąże się to z jakimkolwiek zatwierdzeniem takich metod oceny.

(13) EROD przyjmuje opinię zgodnie z art. 64 ust. 2 RODO w związku z art. 10 ust. 2 regulaminu wewnętrznego EROD w terminie ośmiu tygodni od pierwszego dnia roboczego po podjęciu przez przewodniczącą i właściwy organ nadzorczy decyzji o kompletności dokumentacji. Ze względu na złożony charakter sprawy termin ten można przedłużyć o dalsze sześć tygodni na podstawie decyzji przewodniczącej. Jeżeli z opinii EROD wynika, że nie można zatwierdzić kryteriów, co do których istnieją wątpliwości, ON może ponownie przedłożyć kryteria do zatwierdzenia, gdy wątpliwości wyrażone w pierwotnej opinii EROD zostaną wyeliminowane.

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1. STRESZCZENIE FAKTÓW

1. Zgodnie z art. 42 ust. 5 RODO i wytycznymi projekt „Katalogu kryteriów EuroPriSe do certyfikacji operacji przetwarzania przez podmioty przetwarzające (zakres: UE) v1.5” (dalej „projekt kryteriów certyfikacji”, „kryteria certyfikacji” lub „kryteria”) został sporządzony przez EuroPriSe Cert GmbH (dalej „właściciel systemu”), podmiot prawny z Niemiec, i przedłożony Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, właściwemu niemieckiemu organowi nadzorczemu w Nadrenii Północnej-Westfalii (dalej „ON DE-NRW”).

2. 29 kwietnia 2024 r. organ nadzorczy Niemiec (dalej „ON DE”) przedłożył projekt kryteriów certyfikacji do zatwierdzenia przez EROD zgodnie z art. 64 ust. 2 RODO. 29 maja 2024 r. podjęto decyzję w sprawie kompletności dokumentacji.

3. Mechanizm certyfikacji EuroPriSe nie jest certyfikacją w rozumieniu art. 46 ust. 2 lit. f) RODO przeznaczoną do międzynarodowego przekazywania danych osobowych, a zatem nie zapewnia odpowiednich zabezpieczeń na potrzeby przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach, o których mowa w art. 46 ust. 2 lit. f). Istotnie, wszelkie przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może mieć miejsce tylko wtedy, gdy przestrzegane są przepisy rozdziału V RODO.

2. OCENA

4. EROD przeprowadziła ocenę kryteriów certyfikacji pod kątem ich zatwierdzenia na mocy art. 42 ust. 5 RODO zgodnie ze strukturą przewidzianą w załączniku 2 do wytycznych (dalej „załącznik”) i jego uzupełnieniem.

2.1 Zakres mechanizmu certyfikacji i przedmiot oceny

5. Mechanizm certyfikacji EuroPriSe zawiera kryteria certyfikacji ogólnounijnego systemu certyfikacji na potrzeby certyfikacji przetwarzania przez podmioty przetwarzające. Przedmiotem certyfikacji, do których stosuje się katalog kryteriów, są operacje przetwarzania prowadzone w produktach, procesach i usługach lub z pomocą (również kilku) produktów i usług oraz w odniesieniu do których wnioskodawca ubiegający się o certyfikację występuje w charakterze podmiotu przetwarzającego. Główne kryteria tego mechanizmu certyfikacji dzielą się na trzy zestawy wymogów, mianowicie: z perspektywy prawnej (zestaw 1), z perspektywy środków technicznych i organizacyjnych (zestaw 2) oraz z perspektywy praw osób, których dane dotyczą (zestaw 3).

6. Wnioskodawcy ubiegający się o certyfikację w tym systemie muszą być podmiotami przetwarzającymi. Wymóg ten obejmuje podmioty przetwarzające, którym administrator danych bezpośrednio powierza przetwarzanie danych osobowych w rozumieniu art. 4 ust. 7 RODO. Wnioskodawcami ubiegającymi się o certyfikację mogą być jednak również podmioty przetwarzające w rozumieniu art. 28 ust. 2 i 4 RODO (podwykonawcy przetwarzania).

7. W przypadku gdy podmiot przetwarzający – certyfikowany w systemie certyfikacji EuroPriSe – korzysta z usług podwykonawcy przetwarzania, ten ostatni nie może twierdzić, że uzyskał certyfikację w systemie certyfikacji EuroPriSe. W takim przypadku certyfikacja obejmuje wyłącznie operacje przetwarzania wykonywane przez pierwotny i certyfikowany podmiot przetwarzający. Podwykonawcy przetwarzania mogą jednak również ubiegać się o certyfikację, co skutkuje osobną i niezależną procedurą.

8. EROD zauważa w dokumentacji związanej z zakresem mechanizmu certyfikacji dostarczonej przez ON DE, że system EuroPriSe ma zastosowanie do podmiotów przetwarzających mających jednostkę organizacyjną w Unii Europejskiej (UE) lub w Europejskim Obszarze Gospodarczym (EOG).

2.2 Operacje przetwarzania

9. Zakres tych kryteriów nie ogranicza się do konkretnych rodzajów operacji przetwarzania. Stanowią one raczej metodykę leżącą u podstaw oceny EuroPriSe, która umożliwia certyfikację wszelkich

operacji przetwarzania przez podmioty przetwarzające. Jest to zatem uniwersalne podejście metodyczne, na podstawie którego można certyfikować dużą liczbę bardzo różnych operacji przetwarzania. W związku z tym zasadnicze znaczenie ma przestrzeganie wymogów metodycznych, ponieważ jest to jedyny sposób na zapewnienie jednolitego stosowania kryteriów certyfikacji i porównywalnego poziomu badań w poszczególnych procedurach certyfikacji. Celem jest zapewnienie porównywalności i odtwarzalności wydanych certyfikatów i ich wyników.

2.3 Zgodność z prawem i zasady przetwarzania danych

10. Kryteria wymagają zbadania, czy operacje przetwarzania poddawane certyfikacji są zgodne z zasadą uwzględnienia ochrony danych w fazie projektowania oraz zasadą domyślnej ochrony danych (sekcja 1.5 kryteriów), co wiąże się z udziałem wnioskodawcy, który wspiera administratora we wdrażaniu tych zasad. Umożliwia to ocenę zgodności z art. 25 RODO w związku z art. 5 RODO. Chociaż nie ma kryteriów służących bezpośrednio do zapewnienia zgodności z art. 6 RODO – zważywszy że administrator odpowiada za zgodność przetwarzania z prawem – celem kryteriów jest zapewnienie, aby podmioty przetwarzające-wnioskodawcy projektowali operacje przetwarzania, które są poddawane certyfikacji, w sposób ułatwiający administratorom wdrażanie zasad ochrony danych określonych w art. 5 RODO, w tym zasady zgodności przetwarzania z prawem.

2.4 Ogólne obowiązki administratorów danych i podmiotów przetwarzających

11. Kryteria odzwierciedlają relacje między podmiotem przetwarzającym a administratorem. Kryteria zawierają w szczególności obowiązek posiadania przez podmiot przetwarzający wzoru umowy o przetwarzaniu danych zawieranej z administratorem, obejmującej wszystkie wymogi określone w art. 28 RODO (sekcja 1.2 kryteriów).

12. Kryteria przewidują wymóg, aby wnioskodawcy powołali inspektora ochrony danych (IOD) zgodnie z art. 37 RODO i przedstawili dowód jego powołania (np. zaświadczenie o powołaniu). W ramach kryteriów sprawdza się, czy IOD spełnia wymogi określone w art. 37–39 (zestaw 1, sekcja 1.1 kryteriów).

13. W ramach kryteriów sprawdza się treść rejestrów czynności przetwarzania zgodnie z art. 30 RODO (zestaw 1, sekcja 1.1 kryteriów).

2.5 Prawa osób, których dane dotyczą

14. Kryteria odpowiednio uwzględniają prawo osoby, której dane dotyczą, do bycia poinformowaną zgodnie z rozdziałem III RODO i zawierają wymóg wprowadzenia odpowiednich środków. Przewidziano w nich również konieczność wprowadzenia środków umożliwiających ingerencję w operację przetwarzania na potrzeby zagwarantowania praw osób, których dane dotyczą, oraz umożliwienia sprostowania, usunięcia danych lub ograniczenia ich przetwarzania (zestaw 3 kryteriów).

2.6 Zagrożenia dla praw i wolności

15. Kryteria nakładają na podmiot przetwarzający wymóg świadomości możliwych zagrożeń dla praw i wolności osób fizycznych w związku z przetwarzaniem danych w przedmiocie oceny. W przypadku gdy przetwarzanie danych osobowych może nieść ze sobą wysokie ryzyko dla praw i wolności osób fizycznych, szereg kryteriów służy zapewnieniu, aby wnioskodawca wykazał, że wymogi określone w art. 35 RODO są spełnione zgodnie z art. 35 RODO (sekcja 1.2.2 kryteriów, wymóg nr 6, sekcja 1.3.2 kryteriów, sekcja 1.3.3 kryteriów, sekcja 2.1.5.1 kryteriów, sekcja 2.1.5.9 lit. f) kryteriów).

2.7 Środki techniczne i organizacyjne gwarantujące ochronę

16. Kryteria zawierają wymóg stosowania środków technicznych i organizacyjnych zapewniających poufność, integralność i dostępność operacji przetwarzania. Przewidują również wymóg stosowania środków technicznych służących wdrożeniu ochrony danych już w fazie projektowania oraz domyślnej ochrony danych zgodnie z art. 25 i art. 32 RODO (sekcja 1.5 kryteriów, sekcja 2.1 kryteriów/innych dokumentów).

17. Zgodnie z kryteriami wymaga się zastosowania środka zapewniającego, aby obowiązki związane ze zgłoszeniem naruszenia ochrony danych osobowych wykonywano w odpowiednim czasie i zakresie zgodnie z art. 33 RODO (sekcja 1.2.2 kryteriów, wymóg nr 6).

2.8 Kryteria mające na celu wykazanie istnienia odpowiednich zabezpieczeń na potrzeby przekazywania danych osobowych

18. W kryteriach nałożono wymóg identyfikacji wszystkich przypadków przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych zaangażowanych w przedmiot oceny oraz wymóg uzasadnienia wyboru dokonanego w odniesieniu do mechanizmu przekazywania danych, aby zapewnić odpowiednie zabezpieczenia, zgodnie z rozdziałem V RODO (sekcja 1.4 kryteriów).

3. DODATKOWE KRYTERIA DOTYCZĄCE EUROPEJSKIEGO ZNAKU JAKOŚCI OCHRONY DANYCH

19. Zgodnie z wytycznymi ocena obejmuje pytanie: „czy kryteria są w stanie uwzględnić przepisy lub scenariusze dotyczące ochrony danych w państwach członkowskich”. Sekcja 4 kryteriów zawiera ciążący na wnioskodawcy wymóg przestrzegania obowiązujących krajowych i odpowiednich sektorowych przepisów o ochronie danych. EROD zakłada ponadto, że „sprawozdanie dotyczące zgodności z przepisami prawa krajowego” – oceniające w szczególności zgodność przedmiotu oceny z obowiązującymi krajowymi wymogami prawa o ochronie danych – zostanie sporządzone przez specjalistów prawników, pod warunkiem że wykażą się oni odpowiednim poziomem wiedzy fachowej na temat obowiązującego prawa krajowego.

WNIOSKI/ZALECENIA

20. Podsumowując, EROD uważa, że kryteria certyfikacji są zgodne z RODO, i zatwierdza je zgodnie z zadaniem EROD określonym w art. 70 ust. 1 lit. o) RODO, co skutkuje wspólną certyfikacją (europejskim znakiem jakości ochrony danych).

21. EROD zarejestruje mechanizm certyfikacji „Katalog kryteriów EuroPriSe do certyfikacji operacji przetwarzania przez podmioty przetwarzające” w publicznym rejestrze mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych na podstawie art. 42 ust. 8.

UWAGI KOŃCOWE

22. Niniejsza opinia jest skierowana do niemieckiego organu nadzorczego w Nadrenii Północnej-Westfalii i zostanie podana do wiadomości publicznej zgodnie z art. 64 ust. 5 lit. b) RODO.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca
Anu Talus