Opinia 14/2026 w sprawie kryteriów certyfikacji Europrivacy dotycząca ich zatwierdzenia przez EROD jako europejskiego znaku jakości ochrony danych zgodnie z art. 42 ust. 5 RODO

Przyjęta 15 kwietnia 2026 r.

Spis treści

Europejska Rada Ochrony Danych,

uwzględniając art. 63, art. 64 ust. 2 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 (zwanego dalej „RODO”),

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

uwzględniając art. 10 i 22 swojego regulaminu wewnętrznego,

a także mając na uwadze, co następuje:

1. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych (zwana dalej „EROD”) i Komisja Europejska zachęcają, w szczególności na szczeblu Unii, do ustanawiania mechanizmów certyfikacji w zakresie ochrony danych osobowych (zwanych dalej „mechanizmami certyfikacji”) oraz znaków jakości i oznaczeń w dziedzinie ochrony danych w celu wykazania zgodności z RODO operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające, z uwzględnieniem szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Ponadto ustanowienie mechanizmów certyfikacji może zwiększyć przejrzystość i umożliwić osobom, których dane dotyczą, ocenę stopnia ochrony danych, której podlegają stosowne produkty i usługi.
2. Integralną część mechanizmu certyfikacji stanowią kryteria certyfikacji. W związku z tym w RODO wymaga się 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 (zwany dalej „ON”) zamierza zaproponować zatwierdzenie przez EROD europejskiego znaku jakości ochrony danych zgodnie z art. 42 ust. 5 RODO, ON powinien oświadczyć, że właściciel systemu zamierza oferować 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, w tym przez ON, administratorów i podmioty przetwarzające, w świetle podstawowych elementów, które mechanizmy certyfikacji muszą ustanowić. W szczególności EROD przeprowadza ocenę na podstawie „Wytycznych 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia” (zwanych dalej „wytycznymi”) oraz ich uzupełnienia zawierającego „Wytyczne w sprawie oceny kryteriów certyfikacji” (dalej „uzupełnienie”), dla których okres konsultacji publicznych upłynął 26 maja 2021 r.
5. W związku z tym EROD uznaje, że każdy mechanizm certyfikacji należy rozpatrywać indywidualnie i pozostaje on bez uszczerbku dla oceny każdego innego mechanizmu certyfikacji.
6. Mechanizmy certyfikacji powinny umożliwiać administratorom i podmiotom przetwarzającym wykazanie zgodności z RODO. W związku z tym ich kryteria powinny odpowiednio

[1] Odniesienia do „państw członkowskich” zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG”.

odzwierciedlać wymogi i zasady dotyczące ochrony danych osobowych określone w RODO i przyczyniać się do ich spójnego stosowania.

7. Jednocześnie właściciel systemu powinien zapewnić dostosowanie i zgodność mechanizmu certyfikacji z wszelkimi uwzględnionymi lub zastosowanymi normami ISO i praktykami certyfikacji.

8. W związku z tym certyfikacje powinny stanowić wartość dodaną dla administratorów i podmiotów przetwarzających i pomagać we wdrażaniu znormalizowanych i szczegółowo określonych środków organizacyjnych i technicznych, które wyraźnie ułatwiają i wzmacniają zapewnienie zgodności operacji przetwarzania z RODO, z uwzględnieniem wymogów sektorowych.

9. EROD z zadowoleniem przyjmuje starania podejmowane przez właścicieli systemów mające na celu opracowanie mechanizmów certyfikacji, które są praktycznymi i potencjalnie opłacalnymi narzędziami zapewniającymi większą spójność z RODO oraz wspierającymi prawo do prywatności i ochrony danych osób, których dane dotyczą, przez zwiększenie przejrzystości.

10. EROD przypomina, że certyfikacja jest dobrowolnym narzędziem rozliczalności oraz że stosowanie mechanizmu certyfikacji nie zmniejsza odpowiedzialności administratorów lub podmiotów przetwarzających za zgodność z RODO ani nie uniemożliwia organom nadzorczym wykonywania ich zadań i uprawnień zgodnie z RODO i odpowiednimi przepisami krajowymi.

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

12. Niniejsza opinia EROD dotyczy wyłącznie kryteriów certyfikacji. EROD może wymagać ogólnych informacji na temat metod oceny, aby móc dokładnie ocenić możliwość kontroli kryteriów w kontekście swojej opinii na ten temat. Nie obejmuje to jednak żadnego rodzaju zatwierdzania takich metod oceny.

13. Opinię EROD przyjmuje się 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 uznaniu dokumentacji za kompletną przez przewodniczącą i właściwy organ nadzorczy. Na podstawie decyzji podjętej przez przewodniczącą okres ten może zostać przedłużony o kolejne sześć tygodni z uwagi na złożoność sprawy. Jeżeli w opinii EROD stwierdzi, że nie można zatwierdzić kryteriów, ON może ponownie przedłożyć kryteria do zatwierdzenia po wyeliminowaniu zastrzeżeń wyrażonych w pierwotnej opinii EROD,

przyjmuje niniejszą opinię:

1 Streszczenie faktów

14. Zgodnie z art. 42 ust. 5 RODO i wytycznymi Europejskie Centrum Certyfikacji i Prywatności (zwane dalej „właścicielem systemu”) opracowało 82. wersję kryteriów certyfikacji Europrivacy (zwaną dalej „kryteriami certyfikacji”).

15. 29 stycznia 2026 r. organ nadzorczy Luksemburga (zwany dalej „ON LU”) przedłożył EROD do zatwierdzenia kryteria certyfikacji Europrivacy (wersja 82) zgodnie z art. 64 ust. 2 RODO.

16. Decyzję o uznaniu tej dokumentacji za kompletną podjęto 31 marca 2026 r.

17. EROD przypomina, że 10 października 2022 r. zatwierdziła – przez wydanie opinii EROD 28/2022 – kryteria certyfikacji Europrivacy (wersja 60) jako europejski znak jakości ochrony danych zgodnie z art. 42 ust. 5 RODO („wcześniejsza opinia EROD").

18. Niniejsza opinia dotyczy zmienionej wersji kryteriów certyfikacji Europrivacy (wersja 82). Przede wszystkim EROD zauważa, że w tej wersji kryteriów certyfikacji, która jest obecnie przedkładana EROD, zakres rozszerzono na wnioskodawców podlegających art. 3 ust. 2 RODO i w związku z tym wprowadzono kryterium dotyczące potencjalnego konfliktu z przepisami prawa państwa trzeciego. Ponadto EROD zauważa, że niektóre z kryteriów certyfikacji zatwierdzonych przez EROD w 2022 r. dostosowano, udoskonalono lub sprecyzowano w zmienionej wersji kryteriów certyfikacji Europrivacy (wersja 82). Zmiany te dotyczą w szczególności: wyznaczenia przedstawiciela w EOG oraz realizacji wniosków właściwych organów ochrony danych w EOG; sprawozdania dotyczącego oceny zgodności z zobowiązaniami krajowymi („NOCAR"), dalszego przetwarzania, zabezpieczeń towarzyszących przetwarzaniu szczególnych kategorii danych osobowych, praw osób, których dane dotyczą, zaangażowania podmiotów podprzetwarzających, postępowania w przypadku naruszeń ochrony danych, oceny ryzyka związanego z przetwarzaniem danych oraz polityki i wymogów w zakresie bezpieczeństwa.

19. EROD podkreśla, że zmiana kryteriów certyfikacji zatwierdzonych już w 2022 r. będzie miała wpływ na udzielone dotychczas certyfikacje, a także na trwające procesy certyfikacji. W związku z tym należy w odpowiedni i przejrzysty sposób zarządzać okresem przejściowym między europejskimi znakami jakości ochrony danych wydawanymi zgodnie z kryteriami certyfikacji zatwierdzonymi we wcześniejszej opinii EROD (wersja 60) a tymi wydawanymi zgodnie z kryteriami certyfikacji (wersja 82), ocenionymi w niniejszej opinii. W tym względzie EROD rozumie, na podstawie dokumentacji przedstawionej przez właściciela systemu, że wszystkie trwające procesy certyfikacji muszą zostać zakończone do końca 2026 r., a po tym czasie kryteria certyfikacji zatwierdzone wcześniejszą opinią EROD (wersja 60) nie będą już stosowane do wydawania nowych certyfikatów. Certyfikaty wydane dotychczas pozostaną ważne do końca trzyletniego okresu ważności i zostaną odnowione zgodnie z kryteriami certyfikacji (wersja 82). W związku z tym po końcu roku 2029 kryteria certyfikacji zatwierdzone wcześniejszą opinią EROD (wersja 60) zostaną w pełni zastąpione kryteriami certyfikacji (wersja 82). Ponadto właściciel systemu poda do wiadomości publicznej informacje dotyczące tego planu przejścia. Podczas akredytacji podmiotów certyfikujących mogą być konieczne pewne dostosowania, ale w niniejszej opinii nie odniesiono się do tej kwestii, ponieważ nie wchodzi ona w zakres kompetencji EROD.

20. Ogólny system certyfikacji Europrivacy nie jest przeznaczony do stosowania jako narzędzie do przekazywania danych zgodnie z art. 42 ust. 2 i art. 46 lit. f) RODO. 29 stycznia 2026 r. ON LU przedłożył również EROD do zatwierdzenia zgodnie z art. 64 ust. 2 RODO dodatkowy zestaw kryteriów certyfikacji („Rozszerzenie systemu certyfikacji Europrivacy na potrzeby certyfikacji zgodnie z art. 46 podmiotów odbierających dane"), którego zakres obejmuje administratorów i podmioty przetwarzające spoza EOG, którzy nie podlegają bezpośrednio RODO zgodnie z art. 3 ust. 2 RODO, ale przetwarzają dane osobowe otrzymane od innego administratora danych lub podmiotu przetwarzającego podlegającego RODO. W odniesieniu do tego zestawu kryteriów certyfikacji, które mają być stosowane jako narzędzie do przekazywania danych zgodnie z art. 46 ust. 2 lit. f) RODO, EROD przyjęła opinię 15/2026.

2 Ocena

21. EROD przeprowadziła ocenę kryteriów certyfikacji na potrzeby ich zatwierdzenia na podstawie art. 42 ust. 5 RODO zgodnie ze strukturą przewidzianą w załączniku 2 do wytycznych (zwanym dalej „załącznikiem") i jego uzupełnieniem.

22. W kontekście niniejszej opinii i w celu zatwierdzenia kryteriów certyfikacji EROD oceniła stosowanie i przedmiot oceny – „wstępne kontrole i weryfikacje" (A); kryteria główne określone w RODO dotyczące Europrivacy (G); „kontrole i weryfikacje" dotyczące środków technicznych i organizacyjnych (T), przedstawione wraz z kryteriami certyfikacji.

23. Ponadto EROD zauważa w tym względzie, że „uzupełniające kontrole i weryfikacje kontekstowe"[2], przedstawione wraz z kryteriami certyfikacji zatwierdzonymi we wcześniejszej opinii EROD (wersja 60), mające na celu zapewnienie, aby przetwarzanie danych w ramach przedmiotu oceny było zgodne z wymogami specyficznymi dla danej dziedziny i technologii[3], nie zostały zatwierdzone przez EROD we wcześniejszej opinii, oraz że takie „uzupełniające kontrole i weryfikacje kontekstowe" nie są już zawarte w zaktualizowanej dokumentacji przedstawionej w kontekście niniejszej opinii.

24. EROD zauważa, że – zgodnie z doprecyzowaniami zawartymi w definicjach systemu – odniesienia do „właściwych organów ochrony danych" w całym systemie oznaczają organy ochrony danych w EOG[4].

25. W odniesieniu do definicji prawa państwa trzeciego EROD rozumie, że odnosi się ono do prawa mającego zastosowanie do wnioskodawcy lub do danych osobowych przetwarzanych w ramach przedmiotu oceny w zakresie, w jakim prawo to nie nakłada ograniczeń na prawa do ochrony danych, które wykraczają poza to, co jest konieczne i proporcjonalne w demokratycznym społeczeństwie do ochrony jednego z celów wymienionych w art. 23 ust. 1 RODO, jest proporcjonalne do zamierzonego celu, nie narusza istoty prawa do ochrony danych oraz przewiduje szczególne środki ochrony praw podstawowych i interesów osób, których dane dotyczą.

2.1 Zakres mechanizmu certyfikacji i przedmiot oceny

26. EROD przypomina[5], że system certyfikacji Europrivacy jest systemem ogólnym, ponieważ jest ukierunkowany na szeroki zakres różnych operacji przetwarzania wykonywanych przez administratorów i podmioty przetwarzające z różnych sektorów działalności.

27. EROD z zadowoleniem przyjmuje fakt, że w dokumentacji dotyczącej zakresu tego systemu certyfikacji przekazanej przez ON LU zmieniony system Europrivacy ma zastosowanie do: **(i)** administratorów i podmiotów przetwarzających posiadających jednostkę organizacyjną w Unii Europejskiej (UE) lub w Europejskim Obszarze Gospodarczym (EOG); **(ii)** administratorów i podmiotów przetwarzających posiadających jednostkę organizacyjną poza EOG, którzy podlegają RODO zgodnie z art. 3 ust. 2 RODO, ponieważ oferują towary lub usługi osobom, których dane dotyczą, w EOG albo ponieważ monitorują zachowania osób, których dane

[2] We wcześniejszej opinii EROD nie zatwierdziła „uzupełniających kontroli i weryfikacji kontekstowych".
[3] Wcześniejsza opinia EROD, pkt 7 i 8.
[4] Zob. definicja „właściwego ON" przewidziana w kryteriach Europrivacy: „»Właściwy organ ochrony danych« odnosi się do organów ochrony danych w EOG. Ogólnie rzecz biorąc, odnosi się on do krajowych organów ochrony danych, które są właściwe do egzekwowania zgodności danych osobowych przetwarzanych w ramach przedmiotu oceny. W przypadku certyfikacji zgodnie z art. 46 RODO udzielonej na podstawie RODO podmiotowi odbierającemu dane, właściwym organem ochrony danych jest organ przekazujący dane w EOG, z wyjątkiem składania skargi, w przypadku której właściwy jest dowolny organ w EOG".
[5] Wcześniejsza opinia EROD, pkt 6.

dotyczą, w EOG[6]. Możliwość zastosowania kryteriów określa się w zależności od roli i obowiązków wnioskodawcy.

28. W odniesieniu do wnioskodawców, o których mowa w art. 3 ust. 2 RODO, znajdujących się w państwie trzecim, którzy nie podlegają decyzji stwierdzającej odpowiedni stopień ochrony obejmującej przedmiot oceny, kryterium A.2.1.6 określa warunki, które należy spełnić przy definiowaniu przedmiotu oceny podczas przeglądu ich wniosku o certyfikację. W szczególności przed rozważeniem audytu certyfikacyjnego od podmiotu certyfikującego wymaga się sprawdzenia, czy wnioskodawca jest w stanie wykazać, że przepisy krajowe i praktyka państwa trzeciego nie utrudniają wnioskodawcy przestrzegania wymogów certyfikacyjnych. W przeciwnym razie proces certyfikacji zostanie zatrzymany na etapie składania wniosku.

29. EROD zauważa, że administrator danych może poddać procesowi certyfikacji Europrivacy przedmiot oceny, który podlega współadministrowaniu (kryterium A.2.1.5). EROD pragnie podkreślić, że – w przypadku gdy przedmiot oceny podlega współadministrowaniu – akredytowany podmiot certyfikujący będzie musiał starannie przeprowadzić proces rozpatrywania wniosku, aby zagwarantować, że przedmiot oceny jest istotny i że wnioskodawca ponosi pełną odpowiedzialność za wypełnienie przez przedmiot oceny wszystkich obowiązków wynikających z RODO, co system certyfikacji ma na celu wykazać. W konsekwencji porozumienie zawarte między wnioskodawcą a innymi współadministratorami zaangażowanymi w przedmiot oceny dotyczące ich odpowiedzialności za wypełnienie obowiązków wynikających z RODO może – w zależności od kontekstu czynności przetwarzania w ramach przedmiotu oceny – uniemożliwić wnioskodawcy spełnienie kryteriów certyfikacji.

2.2 Operacje przetwarzania

30. Jak EROD zauważyła we wcześniejszej opinii, kryteria certyfikacji odnoszą się do odpowiednich elementów operacji przetwarzania (danych, systemów i przetwarzania) w odniesieniu do ogólnego zakresu systemu certyfikacji. W szczególności kryteria certyfikacji umożliwiają identyfikację szczególnych kategorii danych zdefiniowanych w art. 9 RODO (sekcja G.2 kryteriów – „Przetwarzanie szczególnych kategorii danych osobowych").

2.3 Zgodność przetwarzania z prawem

31. Jak stwierdziła EROD we wcześniejszej opinii w sprawie już zatwierdzonych kryteriów certyfikacji (wersja 60), kryteria certyfikacji wymagają sprawdzenia zgodności z prawem przetwarzania danych w odniesieniu do każdej indywidualnej operacji przetwarzania w ramach przedmiotu oceny oraz sprawdzenia wymogów dotyczących podstawy prawnej określonej w art. 6 RODO (sekcja G.1 kryteriów – „Zgodność przetwarzania danych z prawem"). W szczególności EROD z zadowoleniem przyjmuje fakt, że zaktualizowane kryteria certyfikacji wymagają, aby zgoda osób, których dane dotyczą, obejmowała każdy cel przetwarzania oraz aby wycofanie zgody nie powodowało szkody dla osoby, której dane dotyczą.

32. Ponadto, jak zauważono we wcześniejszej opinii EROD, kryteria certyfikacji wymagają sprawdzenia konkretnych wymogów dotyczących warunków, na jakich zgodnie z art. 9 ust. 2 RODO dozwolone jest przetwarzanie szczególnych kategorii danych osobowych (sekcja G.2.1 kryteriów – „Przetwarzanie szczególnych kategorii danych osobowych"), oraz

[6] Zob. wytyczne EROD w sprawie terytorialnego zakresu stosowania RODO (art. 3), wersja 2.1, przyjęte 12 listopada 2019 r., sekcja 2.

zapewnienia dodatkowych ograniczeń i zabezpieczeń w odniesieniu do praw i wolności osoby, której dane dotyczą. Kryteria certyfikacji wymagają też sprawdzenia, w stosownych przypadkach, wymogów dotyczących warunków określonych w art. 10 RODO w odniesieniu do przetwarzania danych osobowych dotyczących wyroków skazujących i czynów zabronionych (sekcja G.2.2 kryteriów). W tym względzie EROD z zadowoleniem przyjmuje też fakt, że zaktualizowane kryteria certyfikacji (kryterium G.2.1.3 – „Dodatkowe zabezpieczenia w odniesieniu do przetwarzania szczególnych kategorii danych osobowych") wymagają również od wnioskodawcy wprowadzenia dodatkowych ograniczeń i zabezpieczeń, dostosowanych do szczególnego charakteru danych i związanego z nimi ryzyka, w przypadku przetwarzania szczególnych kategorii danych osobowych.

33. Ponadto w odniesieniu do wnioskodawców, o których mowa w art. 3 ust. 2 RODO, przebywających w państwie trzecim, którzy nie podlegają decyzji stwierdzającej odpowiedni stopień ochrony obejmującej przedmiot oceny, w zaktualizowanych kryteriach certyfikacji od wnioskodawcy wymaga się przedstawienia sprawozdania sporządzonego przez eksperta prawnego zawierającego ocenę tego, czy prawo krajowe i praktyka państwa trzeciego nie uniemożliwiają wypełnienia obowiązków wnioskodawcy w zakresie ochrony danych wynikających z RODO. Ocena ta obejmuje również sprawdzenie, czy prawo krajowe państwa trzeciego nie nakłada na prawa do ochrony danych ograniczeń, które wykraczają poza to, co jest konieczne i proporcjonalne w demokratycznym społeczeństwie do ochrony jednego z celów wymienionych w art. 23 ust. 1 RODO, jest proporcjonalne do zamierzonego celu, nie narusza istoty prawa do ochrony danych oraz przewiduje szczególne środki ochrony praw podstawowych i interesów osób, których dane dotyczą. Należy ją też poddawać przeglądowi w każdym przypadku, gdy zmiany regulacyjne lub organizacyjne mogą utrudniać spełnienie kryteriów lub wpłynąć na przedmiot oceny lub prawa osób, których dane dotyczą, a podmiot certyfikujący powinien zostać o tym poinformowany (kryterium G.1.1.5).

34. W tym kontekście w zaktualizowanych kryteriach certyfikacji wyjaśniono w wytycznych, że „w przypadku gdy wnioskodawca ma jednostkę organizacyjną poza EOG i korzysta z decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do przetwarzania prowadzonego w ramach przedmiotu oceny, zgodność z tym wymogiem można wykazać za pomocą uproszczonego sprawozdania". Zgodnie z tymi kryteriami w takim sprawozdaniu należało ocenić, czy decyzja stwierdzająca odpowiedni stopień ochrony pozostaje w mocy, i udokumentować powody, dla których przedmiot oceny wchodzi w zakres tej decyzji" (kryterium G.1.1.5 lit. F).

2.4 Zasady przetwarzania danych

35. EROD przypomina, że kryteria certyfikacji odpowiednio uwzględniają zasady ochrony danych zgodnie z art. 5 RODO. W szczególności zaktualizowane kryteria certyfikacji rozszerzają i doprecyzowują zasadę ograniczenia celu przez uwzględnienie specjalnego kryterium wymagającego wykazania, że dane osobowe nie są dalej przetwarzane w sposób niezgodny z tymi celami oraz że wszelkie dalsze przetwarzanie należy odrębnie oceniać jako zgodne z prawem i że przeprowadza się i należycie dokumentuje ocenę zgodności celu na potrzeby dalszego przetwarzania danych (kryterium G.1.1.6).

2.5 Ogólne obowiązki administratorów i podmiotów przetwarzających

36. EROD przypomina, że kryteria certyfikacji [7] odzwierciedlają obowiązki administratora, o których mowa w art. 24 RODO (G.4 – „Odpowiedzialność administratora danych"), i wymagają oceny porozumień umownych między podmiotem przetwarzającym a administratorem zgodnie z art. 28 RODO (sekcja G.5 kryteriów – „Podmioty przetwarzające dane lub podmioty podprzetwarzające").

37. Ponadto EROD z zadowoleniem przyjmuje dodanie wymogu, zgodnie z którym kryteria certyfikacji wymagają od wnioskodawcy, o którym mowa w art. 3 ust. 2 RODO, wyznaczenia biura lub przedstawiciela w EOG zgodnie z art. 27 RODO, których dane kontaktowe są dostępne na stronie internetowej wnioskodawcy (kryterium G.4.1.4). EROD przyjmuje do wiadomości te kryteria certyfikacji i przypomina, że zgodnie z RODO nie zawsze stanowi to obowiązek administratorów i podmiotów przetwarzających, w związku z czym należy pamiętać o warunkach określonych w art. 27 RODO.

38. Ponadto EROD zauważa, jak wskazano w jej wcześniejszej opinii, że zgodnie z kryteriami certyfikacji wszyscy wnioskodawcy muszą wyznaczyć inspektora ochrony danych (IOD), nawet w przypadku, gdy zgodnie z art. 37 RODO wnioskodawca nie jest zobowiązany do wyznaczenia IOD. Kryteria służą sprawdzeniu, czy IOD spełnia wymogi określone w art. 37–39 (sekcja G.9 kryteriów – „Inspektor ochrony danych").

39. Kryteria certyfikacji wymagają też sprawdzenia treści rejestrów czynności przetwarzania zgodnie z art. 30 RODO (sekcja G.5.3 kryteriów – „Rejestry czynności przetwarzania"). W tym względzie EROD z zadowoleniem przyjmuje fakt, że w odniesieniu do wnioskodawców, o których mowa w art. 3 ust. 2 RODO, zaktualizowane kryteria certyfikacji wymagają, aby realizowali oni wnioski właściwych organów ochrony danych w EOG i udostępniali im, na żądanie, rejestr czynności przetwarzania (kryterium G.5.3.5).

40. W tym samym duchu EROD zauważa, że uwzględniono pewne dodatkowe kryteria certyfikacji dotyczące zaangażowania podmiotów podprzetwarzających w odniesieniu do wnioskodawców działających w charakterze administratorów lub podmiotów przetwarzających (sekcja G.5.1.2 – „Zaangażowanie podwykonawców przetwarzania"). Rozróżnienie to pozwala lepiej odzwierciedlić podział ról i obowiązków między podmiotami w łańcuchu przetwarzania.

2.6 Prawa osób, których dane dotyczą

41. Podobnie jak we wcześniejszej opinii EROD przypomina, że kryteria certyfikacji odpowiednio uwzględniają prawa osób, których dane dotyczą, do informacji zgodnie z rozdziałem III RODO i wymagają wprowadzenia odpowiednich środków [8]. Kryteria certyfikacji wymagają także wprowadzenia środków umożliwiających interwencję w daną operację przetwarzania, aby zagwarantować prawa osób, których dane dotyczą, oraz umożliwić wykonanie prawa do sprostowania, usunięcia lub ograniczenia przetwarzania danych (sekcja G.3 kryteriów – „Prawa osób, których dane dotyczą").

42. Ponadto EROD z zadowoleniem przyjmuje usprawnienia wprowadzone w kryteriach certyfikacji w odniesieniu do informacji, które mają być przekazywane osobom, których dane dotyczą (sekcja G 3.2 – „Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą" oraz sekcja G.3.3 – „Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą"), sposobów komunikacji

[7] Wcześniejsza opinia EROD, pkt 15.
[8] Wcześniejsza opinia EROD, pkt 19.

z osobami, których dane dotyczą[9], oraz trybu wykonywania praw osób, których dane dotyczą[10] (sekcja G 3.1 – „Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą"), a także prawa dostępu (sekcja G 3.4 – „Prawo dostępu przysługujące osobie, której dane dotyczą"), prawa do usunięcia danych (sekcja G.3.6 – „Prawo do usunięcia danych" („prawo do bycia zapomnianym"), prawa do ograniczenia przetwarzania (kryterium G 3.7.1 – „Prawo do ograniczenia przetwarzania")), obowiązku powiadomienia o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania (kryterium G.3.8.2 – „Obowiązek informowania osób, których dane dotyczą, o odbiorcach, na żądanie"), prawa do sprzeciwu (sekcja G.3.10 – „Prawo do sprzeciwu") oraz prawa do niepodlegania zautomatyzowanemu podejmowaniu decyzji w indywidualnych przypadkach, w tym profilowaniu (sekcja G.3.11 – „Prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji w indywidualnych przypadkach, w tym profilowaniu").

2.7 Ryzyko naruszenia praw i wolności

43. EROD stwierdziła już we wcześniejszej opinii, że kryteria certyfikacji wymagają oceny ryzyka naruszenia praw i wolności osób fizycznych wynikającego z przetwarzania danych w ramach przedmiotu oceny zgodnie z art. 35 RODO (sekcja G.8 kryteriów – „Obowiązek oceny, czy wymagana jest ocena skutków dla ochrony danych")[11].

44. EROD z zadowoleniem przyjmuje zmiany wprowadzone w kryteriach certyfikacji, zgodnie z którymi „wnioskodawca powinien ocenić, stosując powtarzalną metodykę, ryzyko związane z przetwarzaniem, które może mieć wpływ na prawa i wolności osób fizycznych" (sekcja G.6.2.4 – „Ocena ryzyka w odniesieniu do przetwarzania danych").

45. Ponadto EROD z zadowoleniem przyjmuje dalsze uzupełnienia i informacje szczegółowe wprowadzone w kryteriach certyfikacji. Na przykład EROD zauważa dodanie w procesie oceny skutków dla ochrony danych informacji dotyczących sytuacji, w których wnioskodawca nie jest zobowiązany do przeprowadzenia oceny skutków dla ochrony danych (sekcja G.8.2.1 – „Wymogi związane z procesem oceny skutków dla ochrony danych").

2.8 Środki techniczne i organizacyjne gwarantujące ochronę

46. Jak zauważono we wcześniejszej opinii EROD, kryteria certyfikacji wymagają stosowania środków technicznych i organizacyjnych zapewniających poufność, integralność i dostępność operacji przetwarzania. Kryteria te wymagają również stosowania środków technicznych w celu uwzględnienia ochrony danych w fazie projektowania oraz zapewnienia domyślnej ochrony danych zgodnie z art. 25 i 32 RODO (sekcja G.6 kryteriów – „Uwzględnienie ochrony danych w fazie projektowania i domyślna ochrona danych oraz bezpieczeństwo przetwarzania", sekcja G.6.2 kryteriów – „Bezpieczeństwo przetwarzania" i sekcja – „Kryteria T")[12]. W tym względzie EROD z zadowoleniem przyjmuje fakt, że zmienione kryteria

[9] Na przykład kryterium G.3.1.1 – „Obowiązek informowania w zrozumiałym języku" doprecyzowuje informacje na temat przetwarzania danych przekazane przez wnioskodawcę osobie, której dane dotyczą, i wskazuje, że (i) informacje te powinny być przekazywane na piśmie lub w inny sposób, (ii) powinny być dostępne w języku(-ach) urzędowym(-ych) wnioskodawcy oraz (iii) powinny być dostępne w języku osób, których dane dotyczą, do których oferta jest skierowana.

[10] Na przykład kryterium G.3.1.3 – „Zapewnienie właściwego zarządzania prawami osoby, której dane dotyczą, i ich rejestrowania" wymaga obecnie od wnioskodawcy wdrożenia procedury lub mechanizmu służących również do potwierdzenia otrzymania wniosku osobie, której dane dotyczą, oraz do prowadzenia rejestru takich wniosków wraz z datą ich otrzymania.

[11] Wcześniejsza opinia EROD, pkt 20.

[12] Wcześniejsza opinia EROD, pkt 21.

certyfikacji doprecyzowują (sekcja G.6.1.2 – „Domyślna minimalizacja danych") zasady i procedury stosowane przez wnioskodawcę w celu spełnienia tych kryteriów.

47. Jak podkreślono we wcześniejszej opinii EROD, kryteria certyfikacji wymagają stosowania środków mających na celu zapewnienie, aby obowiązki w zakresie zgłaszania naruszeń ochrony danych osobowych były realizowane w odpowiednim czasie i w odpowiednim zakresie zgodnie z art. 33 i 34 RODO (sekcja G.7 kryteriów – „Zarządzanie naruszeniami ochrony danych").

48. W tym względzie EROD zauważa, że kryteria certyfikacji jeszcze bardziej udoskonalono i doprecyzowano. Dokładniej rzecz ujmując, kryteria certyfikacji obejmują obecnie bardziej szczegółowy wykaz (sekcja G.7.1.1 – „Obowiązek dokumentowania naruszeń ochrony danych") informacji, które wnioskodawca musi udokumentować w przypadku wystąpienia naruszenia ochrony danych (np. kategorie danych osobowych, których dotyczy lub może dotyczyć naruszenie, przybliżoną liczbę osób, których dane dotyczą, których dotyczy lub może dotyczyć naruszenie; kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy lub może dotyczyć naruszenie, możliwe konsekwencje naruszenia ochrony danych osobowych).

2.9 Kryteria służące wykazaniu istnienia odpowiednich zabezpieczeń w odniesieniu do przekazywania danych osobowych

49. Jak stwierdziła EROD we wcześniejszej opinii, kryteria certyfikacji wymagają zidentyfikowania wszystkich przypadków przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych objętych przedmiotem oceny oraz uzasadnienia wyboru dokonanego w odniesieniu do mechanizmu przekazywania danych przewidującego odpowiednie zabezpieczenia, zgodnie z rozdziałem V RODO (sekcja G.10 – „Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych").

50. EROD uznaje, że w przypadku wnioskodawców, o których mowa w art. 3 ust. 2 RODO, te kryteria certyfikacji będą miały zastosowanie zarówno w przypadku przekazywania danych osobowych objętych przedmiotem oceny podmiotom mającym siedzibę w tym samym państwie trzecim, w którym znajduje się wnioskodawca, jak i w innym państwie trzecim.

51. Ponadto EROD z zadowoleniem przyjmuje fakt, że kryteria certyfikacji dotyczące przekazywania danych osobowych zostały dopracowane i wyraźniej określają obowiązki wnioskodawcy w tym zakresie (sekcja G.10.1 – „Ogólne obowiązki w zakresie międzynarodowego przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych").

3 Dodatkowe kryteria dotyczące europejskiego znaku jakości ochrony danych

52. Zgodnie z wytycznymi ocena obejmuje pytanie „czy kryteria są w stanie uwzględnić przepisy lub scenariusze dotyczące ochrony danych w państwach członkowskich". Jak stwierdzono we wcześniejszej opinii EROD, w sekcji G.1.1.3 kryteriów certyfikacji wymaga się, aby

wnioskodawca przedstawił taką ocenę w sprawozdaniu dotyczącym oceny zgodności z zobowiązaniami krajowymi (NOCAR). Sprawozdanie takie musi zawierać ocenę zobowiązań krajowych mających zastosowanie do przedmiotu oceny i dokumentować przedsięwzięte przez wnioskodawcę środki na rzecz przestrzegania obowiązujących przepisów oraz ewentualnie bieżące działania naprawcze. Wnioskodawca nie może wykorzystywać wykazu kluczowych uzupełniających wymogów krajowych dostarczonego przez właściciela systemu dla każdego państwa jako wyczerpującego wykazu zobowiązań krajowych istotnych dla przedmiotu oceny. Orientacyjny wykaz minimalnych wymogów dotyczących uzupełniających kontroli i weryfikacji przedstawiony przez właściciela systemu nie stanowi kryteriów certyfikacji objętych zakresem niniejszej opinii.

53. EROD z zadowoleniem przyjmuje dostosowania dokonane w NOCAR w zaktualizowanych kryteriach (sekcja G.1.1.3 – „Ocena zgodności z zobowiązaniami krajowymi"). W szczególności sprecyzowano, że wnioskodawca powinien udokumentować w sprawozdaniu dotyczącym oceny zgodności z zobowiązaniami krajowymi (NOCAR) ocenę zgodności przetwarzania danych „z uzupełniającymi krajowymi zobowiązaniami EOG w zakresie ochrony danych osobowych mającymi zastosowanie do wnioskodawcy". W szczególności NOCAR powinno zawierać m.in. wyraźne określenie przedmiotu oceny, który poddano ocenie, wykaz zidentyfikowanych uzupełniających krajowych zobowiązań EOG w zakresie ochrony danych mających zastosowanie do przedmiotu oceny, a także ocenę zgodności przedmiotu oceny ze zidentyfikowanymi uzupełniającymi krajowymi zobowiązaniami EOG w zakresie ochrony danych. EROD uważa, że w przypadku gdy wnioskodawca ma jednostkę organizacyjną poza EOG i podlega art. 3 ust. 2 RODO, krajowe zobowiązania EOG w zakresie ochrony danych mające zastosowanie do przedmiotu oceny należy określić na podstawie miejsca przebywania osób, których dane dotyczą, którym wnioskodawca oferuje towary lub usługi lub których zachowanie jest monitorowane.

4 Wnioski/zalecenia

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

55. EROD uważa, że kryteria certyfikacji stanowią integralną część systemu certyfikacji i dokona rejestracji systemu certyfikacji Europrivacy w publicznym rejestrze mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także udostępni te kryteria opinii publicznej zgodnie z art. 42 ust. 8 RODO.

5 Uwagi końcowe

56. Niniejsza opinia jest skierowana do ON LU i zostanie podana do wiadomości publicznej zgodnie z art. 64 ust. 5 lit. b) RODO.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

Anu Talus