Opinia 14/2020 w sprawie projektu decyzji właściwego organu nadzorczego Irlandii w sprawie zatwierdzenia wymogów akredytacji podmiotu certyfikującego zgodnie z art. 43 ust. 3 (RODO)

Przyjęta 25 maja 2020 r.

Przyjęta

Spis treści

Europejska Rada Ochrony Danych

uwzględniając art. 63, art. 64 ust. 1 lit. c), art. 64 ust. 3–8 oraz art. 43 ust. 3 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 EOG, a w szczególności jego załącznik XI i protokół 37, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z 6 lipca 2018 r.[1],

uwzględniając art. 10 i 22 swojego regulaminu wewnętrznego z 25 maja 2018 r.,

a także mając na uwadze, co następuje:

1) Głównym zadaniem Rady jest zapewnienie spójnego stosowania rozporządzenia 2016/679 (zwanego dalej „RODO") na całym terytorium Europejskiego Obszaru Gospodarczego. Zgodnie z art. 64 ust. 1 RODO Rada wydaje opinię w przypadku, gdy organ nadzorczy (ON) zamierza zatwierdzić wymogi akredytacji podmiotów certyfikujących na podstawie art. 43. Celem niniejszej opinii jest zatem opracowanie zharmonizowanego podejścia w odniesieniu do wymogów, które organ nadzorczy ds. ochrony danych lub krajowa jednostka akredytująca zastosuje do akredytacji podmiotu certyfikującego. Pomimo że RODO nie nakłada jednolitego zestawu wymogów akredytacji, sprzyja ono spójności. Rada dąży do osiągnięcia tego celu w swoich opiniach, po pierwsze, zachęcając organy nadzorcze do sporządzenia własnych wymogów akredytacji zgodnie ze strukturą określoną w załączniku 1 do wytycznych 4/2018 EROD w sprawie akredytacji podmiotów certyfikujących, a po drugie, analizując je z wykorzystaniem wzoru dostarczonego przez EROD, który umożliwia dokonanie analizy porównawczej tych wymogów (w oparciu o normę ISO 17065 oraz wytyczne EROD w sprawie akredytacji podmiotów certyfikujących).

2) Nawiązując do art. 43 RODO właściwe organy nadzorcze przyjmują wymogi akredytacji. Powinny one jednak zastosować mechanizm spójności, aby wzbudzić zaufanie do mechanizmu certyfikacji, w szczególności poprzez ustanowienie wysokiego poziomu wymogów.

3) Chociaż wymogi akredytacji są objęte mechanizmem spójności, nie oznacza to, że powinny być one identyczne. Właściwe organy nadzorcze posiadają margines swobody w odniesieniu do kontekstu krajowego lub regionalnego i powinny uwzględnić przepisy lokalne. Celem opinii EROD nie jest wypracowanie jednolitego unijnego zbioru wymogów, lecz uniknięcie znaczących niespójności, które mogą mieć wpływ np. na zaufanie do niezależności lub wiedzy fachowej akredytowanych podmiotów certyfikujących.

4) „Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących zgodnie z art. 43 ogólnego rozporządzenia o ochronie danych (2016/679)" (zwane dalej „wytycznymi") oraz „Wytyczne 1/2018 w sprawie certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia 2016/679" posłużą jako wskazówki w kontekście mechanizmu spójności.

[1] Odniesienia do „Unii" w niniejszej opinii należy rozumieć jako odniesienia do „EOG".

5) Jeżeli państwo członkowskie zastrzega sobie, że podmioty certyfikujące mają być akredytowane przez organ nadzorczy, organ ten powinien ustanowić wymogi akredytacji, w tym, ale nie wyłącznie, wymogi wyszczególnione w art. 43 ust. 2 RODO. W porównaniu do zobowiązań związanych z akredytacją podmiotów certyfikujących przez krajowe jednostki akredytujące art. 43 RODO przewiduje mniej szczegółowe wymogi akredytacji w przypadku, gdy dokonuje jej sam organ nadzorczy. Aby przyczynić się do zharmonizowanego podejścia do akredytacji, wymogi akredytacji stosowane przez organ nadzorczy należy oprzeć na normie ISO/IEC 17065 oraz uzupełnić je o dodatkowe wymogi, które organ nadzorczy ustanawia na podstawie art. 43 ust. 1 lit. b) RODO. EROD zauważa, że art. 43 ust. 2 lit. a)–e) RODO odzwierciedlają i precyzują wymogi normy ISO 17065, co przyczyni się do zachowania spójności.[2]

6) Opinia Rady zostaje przyjęta zgodnie z art. 64 ust. 1 lit. c) i art. 64 ust. 3 i 8 RODO w związku z art. 10 ust. 2 regulaminu wewnętrznego EROD w terminie ośmiu tygodni od pierwszego dnia roboczego po podjęciu przez przewodniczącego i właściwy organ nadzorczy decyzji o kompletności dokumentacji. Ze względu na złożony charakter sprawy termin ten można przedłużyć o kolejne sześć tygodni na podstawie decyzji przewodniczącej.

PRZYJMUJE OPINIĘ:

1 STRESZCZENIE STANU FAKTYCZNEGO

1. Irlandzki organ nadzorczy (dalej zwany IE ON) przedłożył EROD swój projekt wymogów akredytacji zgodnie z art. 43 ust. 1 lit. b). Dokumentacja została uznana za kompletną 13 lutego 2020 r. Irlandzka krajowa jednostka akredytująca (IKJA) dokona akredytacji podmiotów certyfikujących, stosując kryteria certyfikacji RODO. Oznacza to, że IKJA zastosuje normę ISO 17065 oraz dodatkowe wymogi ustanowione przez IE ON, po ich zatwierdzeniu przez ten organ, po uzyskaniu opinii Rady w sprawie projektu wymogów akredytacji, aby akredytować podmioty certyfikujące.

2. Zgodnie z art. 10 ust. 2 regulaminu wewnętrznego Rady, ze względu na złożoność rozpatrywanej sprawy, przewodnicząca zdecydowała o przedłużeniu początkowego ośmiotygodniowego terminu o kolejne sześć tygodni.

2 OCENA

2.1 Ogólne uzasadnienie EROD w odniesieniu do przedłożonego projektu decyzji

3. Celem niniejszej opinii jest dokonanie oceny wymogów akredytacji, opracowanych przez ON w związku z normą ISO 17065 lub w formie kompletnego zbioru wymogów, aby umożliwić krajowej jednostce akredytującej lub ON, zgodnie z art. 43 ust. 1 RODO, akredytację podmiotu certyfikującego odpowiedzialnego za dokonywanie i przedłużanie certyfikacji zgodnie z art. 42 RODO. Pozostaje to bez uszczerbku dla zadań i uprawnień właściwego ON. W tym konkretnym przypadku Rada zauważa, że IE

[2] Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych, pkt 39. Dostępne na stronie internetowej: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-42018-accreditation-certification-bodies-under_pl

ON postanowił zwrócić się do swojej krajowej jednostki akredytującej o wydanie akredytacji, po uwzględnieniu dodatkowych wymogów zgodnie z wytycznymi, które powinny zostać zastosowane przez krajową jednostkę akredytującą przy wydawaniu akredytacji.

4. Ocena dodatkowych wymogów akredytacji IE ON ma na celu zbadanie zmian (elementów dodanych lub usuniętych) w odniesieniu do wytycznych, a w szczególności załącznika 1 do wytycznych. Ponadto w opinii EROD skupiono się na wszelkich kwestiach, które mogą mieć wpływ na zachowanie spójnego podejścia w zakresie akredytacji podmiotów certyfikujących.

5. Należy zauważyć, że celem wytycznych w sprawie akredytacji podmiotów certyfikujących jest zapewnienie ON wsparcia przy określaniu ich wymogów akredytacji. Załącznik do wytycznych nie stanowi wymogów akredytacji jako takich. W związku z tym wymogi akredytacji podmiotów certyfikujących muszą zostać określone przez ON w sposób umożliwiający ich praktyczne i spójne zastosowanie, zgodnie z wymaganiami ON.

6. Rada potwierdza fakt, że ze względu na wiedzę fachową krajowych jednostek akredytujących powinny one mieć swobodę działania przy określaniu niektórych przepisów szczególnych w ramach obowiązujących wymogów akredytacji. Rada uznaje jednak za konieczne, by podkreślić, że w przypadku ustanowienia jakichkolwiek dodatkowych wymogów, powinny one zostać określone w sposób umożliwiający ich praktyczne, spójne stosowanie oraz – w razie potrzeby – przegląd.

7. Rada zauważa, że normy ISO, zwłaszcza ISO 17065, podlegają prawom własności intelektualnej, w związku z czym w niniejszej opinii nie będzie odnosić się do ich treści. Rada postanowiła zatem, w stosownych przypadkach, odnieść się do konkretnych sekcji normy ISO, jednakże bez przywoływania jej tekstu.

8. Ponadto Rada dokonała oceny zgodnie ze strukturą przewidzianą w załączniku 1 do wytycznych (zwanym dalej „załącznikiem"). Jeżeli w niniejszej opinii nie odniesiono się do konkretnej sekcji projektu wymogów akredytacji IE ON, należy rozumieć, że Rada nie ma uwag oraz nie wymaga od IE ON podjęcia dalszych działań.

9. Niniejsza opinia nie dotyczy informacji przedłożonych przez IE ON, które są poza zakresem stosowania art. 43 ust. 2 RODO, takich jak odniesienia do przepisów krajowych. Rada zauważa jednak, że przepisy krajowe powinny być zgodne z RODO, jeżeli jest to wymagane.

2.2 Najważniejsze aspekty oceny (art. 43 ust. 2 RODO oraz załącznik 1 do wytycznych EROD), które zgodnie z wymogami akredytacji przewidują spójną ocenę następujących elementów:

1) odniesienie się do wszystkich kluczowych obszarów wskazanych w załączniku do wytycznych, oraz uwzględnienie wszelkich odstępstw od załącznika;

2) niezależność podmiotu certyfikującego;

3) konflikty interesów podmiotu certyfikującego;

4) wiedza fachowa podmiotu certyfikującego;

5) odpowiednie zabezpieczenia zapewniające właściwe stosowanie kryteriów certyfikacji RODO przez podmiot certyfikujący;

6) procedury dotyczące dokonywania, okresowego przeglądu oraz cofania certyfikacji RODO; oraz

7) przejrzyste rozpatrywanie skarg dotyczących naruszeń certyfikacji.

10. Biorąc pod uwagę, że:

a. artykuł 43 ust. 2 RODO zawiera wykaz obszarów akredytacji, które podmiot certyfikujący musi uwzględnić, aby uzyskać akredytację;

b. artykuł 43 ust. 3 RODO stanowi, że wymogi akredytacji podmiotów certyfikujących są zatwierdzane przez właściwy organ nadzorczy;

c. artykuł 57 ust. 1 lit. p) i q) RODO stanowią, że właściwy organ nadzorczy opracowuje i publikuje wymogi akredytacji podmiotów certyfikujących oraz może postanowić o samodzielnym dokonaniu akredytacji podmiotów certyfikujących;

d. artykuł 64 ust. 1 lit. c) RODO stanowi, że Rada wydaje opinię w przypadku, gdy organ nadzorczy zamierza zatwierdzić wymogi akredytacji podmiotu certyfikującego zgodnie z art. 43 ust. 3;

e. jeżeli akredytacji dokonuje krajowa jednostka akredytująca zgodnie z normą ISO/IEC 17065/2012, należy również zastosować dodatkowe wymogi określone przez właściwy organ nadzorczy;

f. w załączniku 1 do wytycznych w sprawie akredytacji certyfikacji przewidziano proponowane wymogi, które organ nadzorczy ds. ochrony danych opracowuje i stosuje podczas akredytacji podmiotu certyfikującego przez krajową jednostkę akredytującą.

Rada jest zdania, że:

2.2.1 PREFIKS (sekcja 0 projektu wymogów akredytacji IE ON)

11. Rada przyznaje, że warunki współpracy, regulujące stosunki między krajową jednostką akredytującą a jej organem nadzorczym ds. ochrony danych, nie są wymogiem akredytacji podmiotów certyfikujących per se. Jednak, w celu zachowania kompletności i przejrzystości, Rada uważa, że takie warunki współpracy, o ile istnieją, podawane są do wiadomości publicznej w formacie, jaki ON uzna za odpowiedni.

2.2.2 TERMINY I DEFINICJE

12. Rada zauważa, że odniesienie do wytycznych w sprawie akredytacji jako „WP 261" nie zostało zaktualizowane. EROD przyjęła wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących zgodnie z art. 43 ogólnego rozporządzenia o ochronie danych (2016/679). W związku z tym Rada zaleca, aby IE ON dokonał zmiany brzmienia oraz odwoływał się do wytycznych 4/2018.

2.2.3 UWAGI OGÓLNE

13. Rada zauważa, że projekt wymogów akredytacji IE ON wielokrotnie odnosi się do „właściwego organu nadzorczego". Ponieważ właściwym organem nadzorczym w tym przypadku jest IE ON, Rada

zachęca, aby organ ten zastąpił to odniesienie określeniem „DPC” lub „IE ON” w celu uniknięcia nieporozumień.

14. Rada zauważa, że projekt wymogów akredytacji IE ON zawiera sekcję poświęconą terminom i definicjom. Niektóre z tych terminów nie są jednak stosowane konsekwentnie w całym dokumencie (np. „przedmiot oceny” i „cel oceny”). Aby uniknąć nieporozumień, Rada zachęca IE ON do stosowania spójnej terminologii w projekcie wymogów.

2.2.4 OGÓLNE WYMOGI AKREDYTACJI (sekcja 4 projektu wymogów akredytacji)

15. Rada uważa, że brzmienie punktu 7 podsekcji 4.1.2 projektu wymogów akredytacji IE ON jest nieco niejasne co do określenia podmiotu, któremu przedstawiane są powody zatwierdzania certyfikacji. Ponadto odniesienie do „ułatwiania” rejestru również nie jest jasne. W związku z tym Rada zachęca, aby IE ON przeredagował je w bardziej przejrzysty sposób.

2.2.5 WYMOGI STRUKTURALNE (sekcja 5 projektu wymogów akredytacji)

16. Rada zauważa, że projekt wymogów akredytacji IE ON odnosi się do powołania „osoby o odpowiednim stażu pracy, odpowiedzialnej za nadzorowanie zgodności z ochroną danych i zarządzaniem informacjami”. Odniesienie do odpowiedniego stażu pracy powinno zostać doprecyzowane pod względem doświadczenia i zakresu uprawnień. Ponadto funkcje tej osoby wydają się podobne do funkcji inspektora ochrony danych. Rada zachęca, aby IE ON jasno określił funkcje pełnione przez tę osobę i doprecyzował na czym polega odpowiednie doświadczenie.

2.2.6 WYMOGI DOTYCZĄCE ZASOBÓW (sekcja 6 projektu wymogów akredytacji)

17. W kwestii personelu podmiotu certyfikującego (podsekcja 6.1), Rada zauważa, że wymogi dla personelu posiadającego techniczną wiedzę fachową i odpowiedzialnego za podejmowanie decyzji, obejmują posiadanie co najmniej pięcioletniego doświadczenia zawodowego związanego z przedmiotem certyfikacji, natomiast personel odpowiedzialny za dokonywanie ocen powinien posiadać co najmniej dwa lata doświadczenia zawodowego. Podobnie personel posiadający prawniczą wiedzę fachową i odpowiedzialny za podejmowanie decyzji musi mieć co najmniej pięć lat doświadczenia zawodowego, natomiast personel odpowiedzialny za dokonywanie ocen musi posiadać co najmniej dwa lata doświadczenia zawodowego. Rada zauważa, że minimalny wymagany okres doświadczenia zawodowego znacznie różni się dla personelu odpowiedzialnego za podejmowanie decyzji i personelu odpowiedzialnego za dokonywanie ocen. W związku z tym Rada uważa, że należy położyć nacisk na inny rodzaj wiedzy fachowej, zamiast na posiadanie konkretnej liczby lat doświadczenia zawodowego. Zdaniem Rady oceniający powinni posiadać bardziej specjalistyczną wiedzę i doświadczenie zawodowe w zakresie procedur technicznych (np. audytów i certyfikacji), natomiast decydenci powinni posiadać bardziej ogólną i kompleksową wiedzę fachową oraz doświadczenie zawodowe w zakresie ochrony danych. W związku z tym Rada zachęca, aby IE ON zwrócił większą uwagę na posiadanie przez oceniających i decydentów zróżnicowanej wiedzy merytorycznej lub doświadczenia zawodowego oraz zmniejszenia różnic w długości wymaganego doświadczenia zawodowego.

2.2.7 WYMOGI DOTYCZĄCE PROCEDUR (sekcja 7 projektu wymogów akredytacji)

18. W odniesieniu do podsekcji 7.10 projektu wymogów akredytacji IE ON („zmiany wpływające na certyfikację”) Rada zauważa, że nie ma odniesienia do procedur zmian, które należy uzgodnić,

zgodnie z sekcją 7.10 załącznika. Rada zachęca, aby IE ON uwzględnił takie odniesienie i wskazał niektóre z procedur, które mogłyby być wprowadzone (np. okresy przejściowe, proces zatwierdzania z właściwym ON...). Ponadto Rada uważa, że również zmiany technologiczne są istotne i mogą mieć wpływ na certyfikację. W związku z tym Rada zachęca, aby IE ON uwzględnił taką możliwość w wykazie zmian mających wpływ na certyfikację. Ponadto Rada z zadowoleniem przyjmuje włączenie naruszeń ochrony danych osobowych i naruszeń RODO do wykazu zmian, które mogą mieć wpływ na certyfikację. W celu zapewnienia przejrzystości Rada zachęca jednak, aby IE ON doprecyzował, że naruszenia ochrony danych lub naruszenia RODO będą brane pod uwagę jedynie w zakresie, w jakim odnoszą się do certyfikacji.

19. W odniesieniu do zmian mających wpływ na certyfikację (podsekcja 7.10 projektu wymogów akredytacji IE ON), a w szczególności podpunktu piątego, Rada zauważa, że IE ON odnosi się do „mających zastosowanie wiążących decyzji Europejskiej Rady Ochrony Danych", a także do art. 39 regulaminu wewnętrznego EROD, który zawiera „wszystkie dokumenty końcowe przyjęte przez EROD". Aby zapewnić pełne zrozumienie znaczenia sformułowania „decyzje Europejskiej Rady Ochrony Danych", Rada zachęca IE ON do jego doprecyzowania. Przykładem może być odniesienie do „dokumentów przyjętych przez Europejską Radę Ochrony Danych".

20. Rada zauważa, że podsekcja 7.11 projektu wymogów akredytacji IE ON (zakończenie, ograniczenie, zawieszenie lub cofnięcie certyfikacji) nie zawiera obowiązku przyjęcia przez podmiot certyfikujący decyzji i zarządzeń IE ON w sprawie cofnięcia lub odmowy dokonania certyfikacji wnioskodawcy, jeżeli wymogi dotyczące certyfikacji nie są już spełniane. W związku z tym Rada zaleca, aby IE ON uwzględnił taki obowiązek.

3 WNIOSKI/ZALECENIA

21. Projekt wymogów akredytacji IE ON może prowadzić do niespójnego stosowania akredytacji podmiotów certyfikujących i konieczne jest wprowadzenie następujących zmian:

22. w odniesieniu do „wymogów dotyczących procedur" Rada zaleca, aby IE ON:

1) Uwzględnił w podsekcji 7.11 obowiązek przyjęcia przez podmiot certyfikujący decyzji i zarządzeń IE ON w sprawie cofnięcia lub odmowy dokonania certyfikacji wnioskodawcy, jeżeli wymogi dotyczące certyfikacji nie są już spełniane.

4 UWAGI KOŃCOWE

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

24. Zgodnie z art. 64 ust. 7 i 8 RODO IE ON w terminie dwóch tygodni po otrzymaniu niniejszej opinii informuje drogą elektroniczną przewodniczącą, czy podtrzymuje projekt wykazu, czy też go zmieni. W powyższym terminie przedstawi zmieniony projekt wykazu lub, w przypadku gdy nie zamierza się zastosować do opinii Rady, poda odpowiednie uzasadnienie niezastosowania się do całości lub części niniejszej opinii.

25. IE ON poinformuje Radę o ostatecznej decyzji w celu włączenia do rejestru decyzji rozpatrywanych w ramach mechanizmu spójności zgodnie z art. 70 ust. 1 lit. y) RODO.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)