czhi

Opinia Rady (art. 64)

Opinia 15/2020 w sprawie projektu decyzji właściwych organów nadzorczych Niemiec 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 załącznik XI do niego i jego 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 z dnia 25 maja 2018 r.,

a także mając na uwadze, co następuje:

(1) Głównym zadaniem Europejskiej Rady Ochrony Danych (EROD) jest zapewnienie spójnego stosowania rozporządzenia 2016/679 (zwanego dalej „RODO") na całym terytorium Europejskiego Obszaru Gospodarczego. Zgodnie z art. 64 ust. 1 RODO Europejska Rada Ochrony Danych wydaje opinię w przypadku, gdy organ nadzorczy (ON) zamierza zatwierdzić wymogi akredytacji podmiotu certyfikującego zgodnie z 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. Europejska Rada Ochrony Danych dąży do osiągnięcia tego celu w swoich opiniach, po pierwsze, zachęcając ON 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) W odniesieniu do art. 43 RODO właściwe organy nadzorcze przyjmują wymogi akredytacji. Powinny one jednak stosować mechanizm spójności, aby wzbudzić zaufanie do mechanizmu certyfikacji, zwłaszcza poprzez ustanowienie wysokiego poziomu wymogów.

(3) Chociaż wymogi akredytacji są objęte mechanizmem spójności, nie oznacza to, że wymogi te powinny być identyczne. Właściwe organy nadzorcze dysponują marginesem swobody w odniesieniu do kontekstu krajowego lub regionalnego i powinny uwzględnić przepisy lokalne. Celem opinii EROD nie jest wypracowanie jednolitego unijnego zestawu 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 na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679)" (zwane dalej „wytycznymi" oraz „Wytyczne 1/2018 w sprawie certyfikacji i określenia 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. W porównaniu z obowiązkami związanymi z akredytacją podmiotów certyfikujących przez krajowe jednostki akredytujące, w art. 43 przewidziano mniej szczegółowych informacji odnośnie do wymogów 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 zgodnie z art. 43 ust. 1 lit. b). EROD zauważa, że art. 43 ust. 2 lit. a) - e) odzwierciedla i precyzuje wymogi normy ISO 17065, co przyczyni się do zachowania spójności[2].

(6) Opinia EROD 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 uznaniu dokumentacji za kompletną przez przewodniczącego i właściwy organ nadzorczy. Okres ten może zostać przedłużony o kolejne 6 tygodni z uwagi na złożoność sprawy, na podstawie decyzji podjętej przez przewodniczącego.

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1 STRESZCZENIE FAKTÓW

1. Niemieckie organy nadzorcze federacji i krajów związkowych (dalej zwane DE ON) przedłożyły EROD swój projekt wymogów akredytacji zgodnie z art. 43 ust. 1 lit. b). Dokumentacja została uznana za kompletną 13 lutego 2020 r. Niemiecka krajowa jednostka akredytująca, DAkkS, dokona akredytacji podmiotów certyfikujących, poświadczając przy tym stosowanie kryteriów certyfikacji zawartych w RODO. Oznacza to, że krajowa jednostka akredytująca będzie stosować normę ISO 17065 oraz dodatkowe wymogi ustanowione przez DE ON, po ich zatwierdzeniu przez te organy w następstwie opinii Europejskiej Rady Ochrony Danych w sprawie projektu wymogów akredytacji, aby akredytować podmioty certyfikujące.
2. Zgodnie z art. 10 ust. 2 regulaminu wewnętrznego Europejskiej Rady Ochrony Danych, ze względu na złożoność rozpatrywanej sprawy, przewodnicząca postanowiła przedłużyć początkowy ośmiotygodniowy termin 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, dokonanie akredytacji podmiotu

[2] Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679), pkt 39. Dostępne tu: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_pl

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 EROD zauważa, że DE ON postanowiły zwrócić się o wspólną akredytację do swojej krajowej jednostki akredytującej, DAkkS oraz właściwego ON, o dokonanie akredytacji, po uwzględnieniu dodatkowych wymogów zgodnie z wytycznymi, które powinny zostać wykorzystane przy dokonywaniu akredytacji.

4. Ocena dodatkowych wymogów akredytacji DE 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 również na wszelkich kwestiach, które mogą mieć wpływ na zachowanie spójnego podejścia w zakresie akredytacji podmiotów certyfikujących.

5. Należy zauważyć, iż 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. Wymogi akredytacji podmiotów certyfikujących muszą zatem zostać określone przez ON w sposób umożliwiający ich praktyczne i spójne stosowanie, zgodnie z wymaganiami kontekstu, w jakim znajdują się ON.

6. EROD przyjmuje do wiadomości fakt, że ze względu na ich wiedzę fachową krajowe jednostki akredytujące oraz, gdzie ma to zastosowanie, również właściwe ON, powinny mieć swobodę działania przy określaniu niektórych przepisów szczególnych w ramach obowiązujących wymogów akredytacji. EROD 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. EROD zauważa, że normy ISO, zwłaszcza ISO 17065, podlegają prawom własności intelektualnej, w związku z czym w niniejszej opinii nie będzie odnosić się do treści powiązanego dokumentu. EROD postanowiła zatem, w stosownych przypadkach, odnieść się do konkretnych sekcji normy ISO, jednakże bez wykorzystywania jej tekstu.

8. Ponadto EROD 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 DE ON, należy rozumieć, że EROD nie ma uwag oraz nie wymaga od DE ON podjęcia dalszych działań.

9. Niniejsza opinia nie dotyczy pozycji przedłożonych przez DE ON, które są poza zakresem stosowania art. 43 ust. 2 RODO, takich jak odniesienia do przepisów krajowych. EROD zauważa jednak, że prawodawstwo krajowe powinno 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 z 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 EROD 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 zawiera proponowane wymogi, które organ nadzorczy ds. ochrony danych opracowuje i stosuje podczas akredytacji podmiotu certyfikującego przez krajową jednostkę akredytującą;

EROD jest zdania, że:

2.2.1 PREFIKS

11. EROD przyznaje, że warunki współpracy, regulujące stosunki między krajową jednostką akredytującą a jej organem nadzorczym ds. ochrony danych, nie stanowią wymogu akredytacji podmiotów certyfikujących *per se*. W celu zachowania kompletności i przejrzystości EROD uznaje jednak, że takie warunki współpracy, o ile istnieją, należy podać do wiadomości publicznej w formacie, jaki ON uzna za odpowiedni.

2.2.2 TERMINY I DEFINICJE

12. EROD zauważa, że rozdział 3 („Definicje“) projektu wymogi akredytacji DE ON określa, jakie rodzaje systemów certyfikacji są dozwolone, precyzując, że muszą one spełniać wymogi normy DIN EN ISO/IEC 17065. W związku z tym należy podkreślić, że w sekcjach 5.1 i 5.2 wytycznych EROD już wyczerpująco określono, co może zostać poddane certyfikacji w ramach RODO. EROD uznaje zatem, że intencją DE SA nie jest ograniczenie tego, co zostało określone w wytycznych oraz że twierdzenia zawarte w

rozdziale 3 projektu wymogów akredytacji DE ON należy uznać za mające zastosowanie w kontekście tych wymogów akredytacji.

2.2.3 UWAGI OGÓLNE

13. EROD zauważa, że w części „uwagi ogólne" projektu wymogów akredytacji DE ON znajduje się odniesienie do „wydania zezwolenia" na kryteria certyfikacji przez EROD „zgodnie z art. 63, art. 64 ust. 1 lit. c) RODO". EROD zwraca uwagę, że RODO nie przyznaje EROD kompetencji do „wydania zezwolenia" na kryteria certyfikacji. Jednakże, zgodnie z wyżej wymienionymi artykułami, EROD może zatwierdzić kryteria certyfikacji. Dlatego też EROD zaleca, aby DE ON usunęły odniesienie do „wydania zezwolenia przez EROD", tak aby projekt był zgodny z brzmieniem RODO.

2.2.4 OGÓLNE WYMOGI AKREDYTACJI (rozdział 4 projektu wymogów akredytacji)

14. W odniesieniu do wymogu odpowiedzialności prawnej (sekcja 4.1 projektu wymogów akredytacji DE ON), EROD zauważa, że w dokumencie uzupełniającym DE ON wyjaśniają, że oczekuje się, iż podmiot certyfikujący będzie posiadał aktualne procedury, a zatem nie ma potrzeby dodawania dalszych wymogów w tym zakresie. EROD uważa jednak, że samo oczekiwanie nie zobowiązuje podmiotu certyfikującego do posiadania takich procedur. Jak ustanowiono w sekcji 4.1.1 załącznika do wytycznych, podmioty certyfikujące posiadają aktualne procedury potwierdzające przestrzeganie obowiązków prawnych określonych w warunkach akredytacji. Ponadto podmiot certyfikujący jest w stanie przedstawić dowody na istnienie procedur i środków zgodnych z RODO, w szczególności w zakresie kontroli i przetwarzania danych osobowych organizacji klienta w ramach procesu certyfikacji. W związku z tym EROD zaleca, aby DE ON zmieniły projekt wymogów w celu dostosowania ich do wytycznych.

15. W odniesieniu do podsekcji 4.1.2.2 projektu wymogów akredytacji DE ON („umowa o certyfikacji"), EROD zauważa, że projekt wymogów akredytacji DE ON nie obejmuje obowiązku zapewnienia pełnej przejrzystości wobec właściwych organów nadzorczych w odniesieniu do procedury certyfikacyjnej, w tym w odniesieniu do kwestii objętych tajemnicą umowną. Ponadto nie ma odniesienia do obowiązku zapewnienia podmiotowi certyfikującemu przez wnioskodawcę dostępu do jego czynności przetwarzania. W związku z tym EROD zaleca, aby DE ON uwzględniły takie obowiązki w swoim projekcie.

16. EROD zauważa, że wyraźne odniesienie do zadań i uprawnień właściwego organu nadzorczego (tiret trzecie w sekcji 4.1.2 załącznika) nie zostało zawarte w podsekcji 4.1.2.2 projektu wymogów akredytacji DE ON. EROD jest zdania, że odniesienie to powinno zostać dodane w projekcie wymogów i w związku z tym zaleca, aby DE ON wprowadziły odpowiednie zmiany w treści projektu.

17. Ponadto projekt wymogów DE ON dotyczący umowy o certyfikacji nie obejmuje obowiązku umożliwienia podmiotowi certyfikującemu ujawnienia wszystkich informacji niezbędnych do przyznania certyfikacji zgodnie z art. 42 ust. 8 i art. 43 ust. 5 RODO (tiret siódme w sekcji 4.1.2 załącznika). Mimo że obowiązek ten jest uwzględniony w części dotyczącej zarządzania procesem w projekcie wymogów akredytacji DE ON, EROD uważa, że powinien on stanowić część umowy o certyfikacji, aby wzmocnić jego wiążący charakter. W związku z tym EROD zaleca, aby DE ON uwzględniły powyższy obowiązek jako część elementów umowy o certyfikacji.

18. Zgodnie z załącznikiem wnioskodawca jest zobowiązany poinformować podmiot certyfikujący o istotnych zmianach w jego sytuacji faktycznej lub prawnej oraz o zmianach produktów, procesów i

usługach objętych certyfikacją (tiret dziesiąte w sekcji 4.1.2 załącznika). Jednakże w projekcie wymogów akredytacji DE ON, tiret szóste podsekcji 4.1.2.2 zawiera jedynie obowiązek informowania podmiotu certyfikującego o istotnych zmianach w okolicznościach faktycznych lub prawnych, ale nie wymienia wyraźnie produktów, procesów i usług. EROD zaleca, aby DE ON zawarły takie odniesienie, zgodnie z załącznikiem.

19. W odniesieniu do podsekcji 4.2.7 projektu wymogów akredytacji DE ON („zapewnienie bezstronności"), EROD zaleca wzmocnienie kryteriów mających zastosowanie do podmiotów certyfikujących, które należą do odrębnego podmiotu prawnego lub są przez niego kontrolowane, tak aby uwzględnić fakt, że każdy rodzaj stosunków gospodarczych między podmiotem certyfikującym a podmiotem prawnym, w zależności od jego cech, może wpływać na bezstronność jego działalności certyfikacyjnej.

20. W odniesieniu do sekcji 4.6 projektu wymogów akredytacji DE ON („informacje dostępne publicznie"), EROD zauważa, że brakuje odniesienia do publikacji wszystkich wersji zatwierdzonych kryteriów i procedur certyfikacji. W związku z tym EROD zachęca DE ON do zmiany projektu wymogów akredytacji w celu wyraźnego zaznaczenia, że publikacja obejmuje wszystkie wersje zatwierdzonych kryteriów i procedur certyfikacji. Dodatkowo EROD zwraca uwagę, że drugi akapit sekcji 4.6 stanowi, że „systemy certyfikacji stosowane przez podmiot certyfikujący zatwierdzone kryteria zgodnie z art. 42 ust. 5 RODO, określającym dopuszczalny okres stosowania, *mają być ogólnie publikowane*." Aby uniknąć wszelkich niejasności, EROD zachęca DE ON do skreślenia słowa „ogólnie" i włączenia „oraz" pomiędzy „podmiot certyfikujący" a „zatwierdzone kryteria".

2.2.5 WYMOGI DOTYCZĄCE ZASOBÓW (rozdział 6 projektu wymogów akredytacji)

21. W odniesieniu do wymogów w zakresie wiedzy fachowej, a w szczególności podsekcji 6.1.2.1 projektu wymogów akredytacji DE ON („kompetencje w zakresie zasobów ludzkich"), EROD zauważa, że zapis dotyczący wymaganej wiedzy w wymienionych obszarach nie określa, że wiedza ta jest odpowiednia. W celu zapewnienia spójności z poziomem wiedzy fachowej wymaganym w załączniku, EROD zaleca, aby DE ON dostosowały tekst do wytycznych, wymagając, aby wiedza ta była odpowiednia.

22. Ponadto EROD zauważa, że wymogi w stosunku do pracowników posiadających fachową wiedzę techniczną odpowiedzialnych za podejmowanie decyzji obejmują co najmniej 7 lat doświadczenia zawodowego lub 5 lat doświadczenia zawodowego w zakresie technicznej ochrony danych, w zależności od poziomu ich wykształcenia, natomiast pracownicy odpowiedzialni za przeprowadzanie ocen powinni posiadać 4 lata doświadczenia zawodowego lub 2 lata doświadczenia zawodowego w zakresie technicznej ochrony danych i doświadczenie w zakresie procedury badań, w zależności od poziomu ich wykształcenia. Podobnie personel posiadający prawniczą wiedzę fachową i odpowiedzialny za podejmowanie decyzji musi mieć co najmniej pięć lat doświadczenia zawodowego w zakresie przepisów o ochronie danych, natomiast personel odpowiedzialny za dokonywanie ocen musi posiadać co najmniej dwa lata doświadczenia zawodowego w zakresie przepisów o ochronie danych i procedur audytowych. EROD 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 EROD uważa, że wymogi dotyczące kompetencji oceniających i decydentów powinny być dostosowane do różnych zadań, które wykonują, a nie do liczby lat doświadczenia. Zdaniem EROD 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 EROD zachęca, aby DE ON zwróciły większą uwagę na posiadanie przez oceniających i decydentów zróżnicowanej wiedzy merytorycznej lub doświadczenia zawodowego oraz zmniejszenie różnic w długości wymaganego doświadczenia zawodowego.

23. Ponadto EROD uważa, że wiedza na temat systemów zarządzania istotnych dla obszaru certyfikacji powinna zostać rozszerzona na ISO/IEC 27701:2019 - Techniki bezpieczeństwa – Rozszerzenie na ISO/IEC 27001 i ISO/IEC 27002 w zakresie zarządzania informacjami dotyczącymi prywatności – Wymagania i wytyczne oraz zachęca DE ON do uwzględnienia takiego odniesienia.

24. Dodatkowo, w zakresie wymogów dotyczących wykształcenia personelu technicznego, EROD uważa, że wykaz przedmiotów jest już dostosowany do wiedzy technicznej wymaganej w załączniku. W związku z tym EROD zachęca DE ON do usunięcia odniesienia do „nauk przyrodniczych" z listy przedmiotów dotyczących kształcenia uniwersyteckiego personelu technicznego.

2.2.6 WYMOGI DOTYCZĄCE PROCEDUR (rozdział 7 projektu wymogów akredytacji)

25. EROD zauważa, że rozdział 7 projektu wymogów akredytacji DE ON zawiera kilka odniesień do terminu „kryteria" (np. w sekcjach 7.4, 7.6, 7.11 i 7.13). W celu uniknięcia wszelkich niejasności, EROD zachęca DE ON do wyjaśnienia znaczenia tego terminu, na przykład poprzez dodanie wyjaśnienia w załączniku 1 (glosariusz).

26. W odniesieniu do sekcji 7.1 projektu wymogów akredytacji DE ON („informacje ogólne") EROD zauważa, że brakuje wyraźnego odniesienia do obowiązku spełnienia dodatkowych wymogów przez podmiot certyfikujący. Mimo że taki obowiązek można wywnioskować z tekstu projektu wymogów, EROD uważa, że należy zamieścić wyraźne odniesienie do wyżej wymienionego obowiązku. W związku z tym EROD zaleca, aby DE ON zmieniły odpowiednio projekt.

27. EROD zauważa, że projekt dodatkowych wymogów DE ON nie zawiera żadnego odniesienia do funkcjonowania zatwierdzonego europejskiego znaku jakości ochrony danych, zgodnie z sekcją 7.1.2 załącznika. EROD jest zdania, że odniesienie to powinno zostać uwzględnione, w szczególności biorąc pod uwagę, że akredytacja podmiotu certyfikującego przyznającego europejskie znaki jakości ochrony danych może być konieczna w każdym z państw członkowskich, w których podmiot certyfikujący ma jednostkę organizacyjną.[3] W związku z tym EROD zaleca, aby DE ON zmieniły odpowiednio wyżej wymienione odniesienie. Na przykład projekt wymogów mógłby zawierać, co następuje: *„Właściwy organ nadzorczy jest powiadamiany przed rozpoczęciem przez podmiot certyfikujący obsługi zatwierdzonego europejskiego znaku jakości ochrony danych w nowym państwie członkowskim z właściwego oddziału".*

28. EROD zauważa, że w sekcji 7.2 („wniosek") projekt wymogów akredytacji DE ON przewiduje sytuację, w której podmioty przetwarzające są wykorzystywane do przeprowadzania operacji przetwarzania danych, zgodnie z załącznikiem do wytycznych. EROD zauważa jednak, że w przypadku korzystania z usług podmiotów przetwarzających wniosek zawiera odpowiednią umowę (umowy) z administratorem/podmiotem przetwarzającym, zgodnie z załącznikiem. W związku z tym EROD zaleca, aby DE ON dostosowały brzmienie do wytycznych poprzez zamieszczenie odniesienia do umowy (umów) z administratorem/podmiotem przetwarzającym. Ponadto EROD zachęca DE ON do

[3] W związku z tym zob. wytyczne 1/2018, ust. 44.

rozważenia, czy w tym przypadku należy również wspomnieć o wspólnych administratorach i ich szczególnych uzgodnieniach.

29. EROD zauważa, że sekcja 7.2 projektu wymogów akredytacji DE ON określa, iż „administrator i podmiot przetwarzający są uprawnieni do ubiegania się o certyfikację". Możliwość składania wniosków o certyfikację przez podmioty przetwarzające będzie zależała od konkretnego systemu certyfikacji. W związku z tym, aby uniknąć nieporozumień, EROD zachęca DE ON do usunięcia powyższego odniesienia lub do wyjaśnienia, że możliwość uzyskania certyfikatu przez podmioty przetwarzające będzie zależała od zakresu systemu certyfikacji.

30. W odniesieniu do sekcji 7.3 projektu wymogów akredytacji DE ON („wnioski o ocenę"), EROD odnotowuje, że projekt wymogów akredytacji DE ON stwierdza, iż „planowane metody oceny będą określane w umowie [...]". W celu wyjaśnienia, że jest to wymóg, EROD zachęca DE ON do przeredagowania pierwszego akapitu w celu wyjaśnienia, że metody oceny są zawarte w umowie o certyfikacji, tzn. przeredagować wymóg na „zaplanowane metody oceny są określone w umowie [...]". Ponadto EROD zachęca DE ON do zastąpienia odniesienia do pkt 7.3.1.b normy ISO 17065 odniesieniem do pkt 7.3 normy ISO 17065, w celu ujednolicenia brzmienia z załącznikiem. Ponadto EROD zauważa, że akapit czwarty odnosi się do właściwych kompetencji technicznych i prawnych. W celu zapewnienia jasności EROD zachęca DE ON do dodania w „dziedzinie ochrony danych".

31. EROD zauważa, że punkt 7.4 projektu wymogów akredytacji DE ON („metody oceny") nie zawiera obowiązku opisania przez podmiot certyfikujący wystarczających metod oceny dla oceny zgodności operacji przetwarzania z kryteriami certyfikacji. EROD zaleca, aby DE ON zmieniły projekt wymogów w celu zawarcia takiego odniesienia. Przykładem może być dodanie następujących elementów: *„Podmiot certyfikujący zapewni, że mechanizmy stosowane do przyznawania certyfikacji będą opisywać wystarczające metody oceny zgodności operacji przetwarzania z kryteriami certyfikacji*". Ponadto w odniesieniu do pierwszego obszaru, który zostanie objęty metodami oceny, EROD uważa, że konieczność (niezbędność) i proporcjonalność są oceniane również w odniesieniu do zainteresowanych osób, których dane dotyczą, w stosownych przypadkach. Na koniec EROD zauważa brak odniesienia do dokumentacji metod i ustaleń. EROD zaleca zatem, aby DE ON zmieniły projekt wymogów w celu zawarcia takiego odniesienia.

32. W odniesieniu do istniejących certyfikatów (sekcja 7.4 projektu wymogów akredytacji DE ON) EROD uważa, że tiret czwarte na stronie 13 prowadzi do nieporozumień, ponieważ nie jest jasne, jaki jest związek między okresami ważności obecnej i poprzedniej certyfikacji oraz w jaki sposób miałyby one do siebie pasować. Ponadto nie wydaje się możliwe zakwestionowanie ważności certyfikacji wydanej wcześniej przez inny akredytowany podmiot certyfikujący. Podsumowując, akapit ten zyskałby w pewnym stopniu na jasności w odniesieniu do relacji między poszczególnymi elementami. EROD zaleca, aby DE ON wprowadziły zmiany do projektu, w szczególności poprzez wyjaśnienie, że okres ważności certyfikatu RODO nie może być uzależniony od ważności innych rodzajów certyfikatów.

33. W odniesieniu do sekcji 7.5 („oszacowanie") projektu wymogów akredytacji DE ON, EROD zachęca DE ON do zmiany tytułu sekcji na „przegląd".

34. W odniesieniu do zmian mających wpływ na certyfikację (sekcja 7.10 projektu wymogów akredytacji DE ON), EROD zauważa, że projekt wymogów akredytacji DE ON stanowi, że „klient jest informowany w odpowiednim czasie o zmianach w zakresie ram prawnych, które go dotyczą". Mając na uwadze potrzebę zachowania bezstronności podmiotu certyfikującego, EROD zachęca DE ON do przeformułowania zdania, aby wyjaśnić, że klient otrzymuje w odpowiednim czasie ogólne informacje o zmianach, które mogą go dotyczyć. Dodatkowo, aby zapewnić pełne zrozumienie znaczenia

sformułowania „decyzje Europejskiej Rady Ochrony Danych”, EROD zachęca DE ON do wyjaśnienia odniesienia. Przykładem może być odniesienie do „dokumentów przyjętych przez Europejską Radę Ochrony Danych”.

35. EROD zauważa, że sekcja 7.11 projektu wymogów akredytacji DE ON („zakończenie, zawężenie, zawieszenie lub cofnięcie certyfikacji”) nie zawiera obowiązku przyjęcia przez podmiot certyfikujący decyzji i zarządzeń DE ON w sprawie cofnięcia lub odmowy dokonania certyfikacji wnioskodawcy, jeżeli wymogi dotyczące certyfikacji nie są już spełniane. W związku z tym EROD zaleca, aby DE ON uwzględniły taki obowiązek. Ponadto EROD zachęca DE ON do zastąpienia słowa „zawężenie“ słowem „ograniczenie“ w tytule sekcji, zgodnie z załącznikiem do wytycznych.

2.2.7 DALSZE DODATKOWE WYMOGI

36. W odniesieniu do podsekcji 8.11.3 wymogów akredytacji DE ON („obsługa skarg“), EROD zachęca DE ON do zastąpienia odniesienia do „usprawiedliwionych skarg“ odniesieniem do „uzasadnionych skarg“, w celu zapewnienia większej jasności.

3 WNIOSKI/ZALECENIA

37. Projekt wymogów akredytacji niemieckich organów nadzorczych federacji i krajów związkowych może prowadzić do niespójnego stosowania akredytacji podmiotów certyfikujących, dlatego konieczne jest wprowadzenie następujących zmian:

38. w odniesieniu do „uwag ogólnych” EROD zaleca, aby DE ON:

    1) usunęły odniesienie do „wydania zezwolenia przez EROD“, tak aby projekt był zgodny z brzmieniem RODO.

39. w odniesieniu do „ogólnych wymogów akredytacji” EROD zaleca, aby DE ON:

    1) zmieniły wymogi dotyczące odpowiedzialności prawnej (podsekcja 4.1) w celu dostosowania ich do wytycznych.

    2) zmieniły podsekcję 4.1.2.2 w celu włączenia do umowy o certyfikacji obowiązku zapewnienia pełnej przejrzystości dla DE ON w odniesieniu do procedury certyfikacyjnej oraz zapewnienia podmiotowi certyfikującemu dostępu do czynności przetwarzania wnioskodawcy.

    3) zawarły w podsekcji 4.1.2.2 wyraźne odniesienie do zadań i uprawnień właściwego ON, zgodnie z załącznikiem.

    4) zawarły wśród elementów umowy o certyfikacji obowiązek umożliwienia podmiotowi certyfikującemu ujawnienia wszystkich informacji niezbędnych do przyznania certyfikacji zgodnie z art. 42 ust. 8 i art. 43 ust. 5 RODO.

    5) zawarły wyraźne odniesienie do „produktów, procesów i usług, których dotyczy certyfikacja“ w tiret szóstym podsekcji 4.1.2.2.

    6) wzmocniły, w podsekcji 4.2.7, kryteria mające zastosowanie do podmiotów certyfikujących, które należą do odrębnego podmiotu prawnego lub są przez niego

kontrolowane, tak aby uwzględnić fakt, że każdy rodzaj stosunków gospodarczych między podmiotem certyfikującym a podmiotem prawnym, w zależności od jego cech, może wpływać na bezstronność jego działalności certyfikacyjnej.

40. w odniesieniu do „wymogów dotyczących zasobów" EROD zaleca, aby DE ON:

    1) dostosowały treść podsekcji 6.1.2.1 do wytycznych, wymagając, aby wiedza ta była odpowiednia.

41. w odniesieniu do „wymogów dotyczących procedur" EROD zaleca, aby DE ON:

    1) zmieniły sekcję 7.1, tak aby zawierała ona wyraźne odniesienie do obowiązku podmiotu certyfikującego w zakresie spełniania dodatkowych wymogów.

    2) zawarły odniesienie do działania zatwierdzonego europejskiego certyfikatu ochrony danych.

    3) dostosowały sformułowania w sekcji 7.2 do wytycznych poprzez włączenie odniesienia do umowy (umów) administratora/podmiotu przetwarzającego.

    4) zawarły w sekcji 7.4 obowiązek podmiotu certyfikującego do opisania wystarczających metod oceny zgodności operacji przetwarzania z kryteriami certyfikacji.

    5) wyjaśniły w sekcji 7.4, że okres ważności certyfikatu RODO nie może być uzależniony od ważności innych rodzajów certyfikatów.

    6) uwzględniły w podsekcji 7.11 obowiązek przyjęcia przez podmiot certyfikujący decyzji i zarządzeń DE ON w sprawie cofnięcia lub odmowy wydania certyfikacji wnioskodawcy, jeżeli wymogi dotyczące certyfikacji nie są już spełniane.

4 UWAGI KOŃCOWE

42. Niniejsza opinia skierowana jest do niemieckich organów nadzorczych federacji i krajów związkowych i zostanie podana do wiadomości publicznej zgodnie z art. 64 ust. 5 lit. b) RODO.

43. Zgodnie z art. 64 ust. 7 i 8 RODO DE ON w terminie dwóch tygodni po otrzymaniu niniejszej opinii informują drogą elektroniczną przewodniczącego, czy podtrzymują projekt decyzji, czy też go zmienią. W powyższym terminie przedstawią one zmieniony projekt decyzji lub, w przypadku gdy nie zamierzają się zastosować do opinii EROD, podadzą odpowiednie uzasadnienie niezastosowania się do całości lub części niniejszej opinii.

44. DE ON poinformuje EROD 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)

Przyjęta