Wytyczne

Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679)

Wersja 3.0

4 czerwca 2019 r.

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Przyjęte

Historia wersji

Wersja 3.0	4 czerwca 2019 r.	Dodanie załącznika 1 (wersja 2.0 załącznika 1 przyjęta w dniu 4 czerwca 2019 r. po konsultacjach publicznych)
Wersja 2.0	4 grudnia 2018 r.	Przyjęcie wytycznych po konsultacjach publicznych. W tym samym dniu przyjęto załącznik 1 (wersja 1.0) do konsultacji publicznych
Wersja 1.0	6 lutego 2018 r.	Przyjęcie wytycznych przez Grupę Roboczą Art. 29 (wersja do konsultacji publicznych) Tę wersję zatwierdziła Europejska Rada Ochrony Danych w dniu 25 maja 2018 r.

Spis treści

uwzględniając art. 70 ust. 1 lit. e) 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,

biorąc pod uwagę wyniki przeprowadzonych w lutym 2018 r. konsultacji publicznych w sprawie wytycznych oraz wyniki przeprowadzonych między 14 grudnia 2018 r. a 1 lutego 2019 r. konsultacji publicznych w sprawie załącznika, zgodnie z art. 70 ust. 4 ogólnego rozporządzenia o ochronie danych,

PRZYJMUJE NINIEJSZE WYTYCZNE:

1 WPROWADZENIE

1. Ogólne rozporządzenie o ochronie danych (rozporządzenie (UE) 2016/679) („RODO"), które wchodzi w życie dnia 25 maja 2018 r., zapewnia nowoczesne ramy zgodności dotyczące ochrony danych w Europie, oparte na rozliczalności i prawach podstawowych. Podstawę nowych ram stanowi szereg środków służących ułatwieniu zachowania zgodności z przepisami RODO. Obejmują one obowiązkowe wymogi w szczególnych okolicznościach (w tym wyznaczenie inspektorów ochrony danych i prowadzenie oceny skutków dla ochrony danych) i dobrowolne środki, takie jak kodeksy postępowania i mechanizmy certyfikacji.

2. W ramach ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych, w art. 43 ust. 1 RODO wymaga się od państw członkowskich zapewniania, aby podmioty certyfikujące dokonujące certyfikacji na podstawie art. 42 ust. 1 podlegały akredytacji właściwego organu nadzorczego lub krajowej jednostki akredytującej, lub obu tych podmiotów. Jeżeli akredytacji dokonuje krajowa jednostka akredytująca zgodnie z ISO/IEC 17065/2012, należy zastosować również dodatkowe wymogi określone przez właściwy organ nadzorczy.

3. Zrozumiałe mechanizmy certyfikacji mogą przyczynić się do poprawy przestrzegania RODO i zwiększenia przejrzystości dla osób, których dane dotyczą, oraz w relacjach między przedsiębiorcami (B2B), np. między administratorami a podmiotami przetwarzającymi. Administratorzy danych i podmioty przetwarzające dane będą korzystały z poświadczenia niezależnych stron trzecich, aby wykazać zgodność swoich operacji przetwarzania[1].

4. W tym kontekście Europejska Rada Ochrony Danych uznaje, że konieczne jest zapewnienie wytycznych dotyczących akredytacji. Szczególna wartość akredytacji oraz jej cel wynikają z tego, że stanowi ona wiarygodne stwierdzenie właściwości podmiotów certyfikujących, które pozwala na budowanie zaufania względem mechanizmu certyfikacji.

[1] Motyw 100 RODO stanowi, że ustanowienie mechanizmów certyfikacji może zwiększyć przejrzystość i poprawić przestrzeganie rozporządzenia oraz pozwolić w ten sposób osobom, których dane dotyczą, ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi.

5. Celem wytycznych jest dostarczenie wskazówek dotyczących sposobu interpretowania i wdrażania przepisów art. 43 RODO. Mają one w szczególności na celu pomóc państwom członkowskim, organom nadzorczym i krajowym jednostkom akredytującym w ustanowieniu spójnego i jednolitego scenariusza odniesienia dotyczącego akredytacji podmiotów certyfikujących, które dokonują certyfikacji zgodnie z RODO.

2 ZAKRES WYTYCZNYCH

6. W niniejszych wytycznych:

- określono cel akredytacji w kontekście RODO;
- wyjaśniono dostępne sposoby akredytacji podmiotów certyfikujących zgodnie z art. 43 ust. 1 i określono główne kwestie, które należy rozważyć;
- zapewniono ramy służące ustanowieniu dodatkowych wymogów dotyczących akredytacji w sytuacjach, gdy dokonuje jej krajowa jednostka akredytująca; oraz
- zapewniono ramy służące ustanowieniu wymogów dotyczących akredytacji w sytuacjach, gdy dokonuje jej organ nadzorczy.

7. Niniejsze wytyczne nie są podręcznikiem procedur dotyczących akredytacji podmiotów certyfikujących zgodnie z RODO. Nie opracowano w nich nowych norm technicznych w zakresie akredytacji podmiotów certyfikujących do celów RODO.

8. Niniejsze wytyczne są skierowane do:

- państw członkowskich, które muszą zapewnić, aby akredytacji podmiotów certyfikujących dokonywały organ nadzorczy lub krajowa jednostka akredytująca;
- krajowych jednostek akredytujących, które dokonują akredytacji podmiotów certyfikujących na podstawie art. 43 ust. 1 lit. b);
- właściwego organu nadzorczego określającego dodatkowe wymogi oprócz wymogów zawartych w ISO/IEC 17065/2012[2], gdy akredytacji dokonuje krajowa jednostka akredytująca na podstawie art. 43 ust. 1 lit. b);
- Europejskiej Rady Ochrony Danych, która wydaje opinię na temat wymogów właściwego organu nadzorczego dotyczących akredytacji zgodnie z art. 43 ust. 3, art. 70 ust. 1 lit. p) i art. 64 ust. 1 lit. c) oraz zatwierdza takie wymogi;
- właściwego organu nadzorczego określającego wymogi dotyczące akredytacji, gdy dokonuje jej organ nadzorczy zgodnie z art. 43 ust. 1 lit. a);
- innych zainteresowanych stron, takich jak potencjalne podmioty certyfikujące lub właściciele systemów certyfikujących określający kryteria i procedury certyfikacji[3].

[2] Międzynarodowa Organizacja Normalizacyjna: ocena zgodności – wymogi dotyczące podmiotów certyfikujących produkty, procesy i usługi.

[3] Właścicielem systemu jest możliwa do zidentyfikowania organizacja, która określiła kryteria certyfikacji i wymogi, względem których dokonuje się oceny zgodności. Akredytacja dotyczy organizacji, która przeprowadza ocenę (art. 43 ust. 4) względem wymogów systemu certyfikacji i dokonuje certyfikacji (tj. podmiotu certyfikującego znanego również jako jednostka oceniająca zgodność). Organizacja dokonująca oceny może być tą samą organizacją, która opracowała system i jest jej właścicielem, mogą jednak istnieć ustalenia,

9. Definicje

10. Następujące definicje mają na celu promowanie wspólnego rozumienia podstawowych elementów procesu akredytacji. Należy je traktować jako punkty odniesienia, przy czym nie są one niepodważalne. Definicje te opierają się na istniejących ramach regulacyjnych i normach, szczególnie na odpowiednich przepisach RODO i ISO/IEC 17065/2012.

11. Do celów niniejszych wytycznych mają zastosowanie następujące definicje:

12. *akredytacja* podmiotów certyfikujących – zob. sekcja 3 dotycząca interpretacji akredytacji dla celów art. 43 RODO;

13. *dodatkowe wymogi* oznaczają wymogi ustanowione przez właściwy organ nadzorczy, względem którego dokonuje się akredytacji[4];

14. *certyfikacja* oznacza ocenę i bezstronne potwierdzenie przez stronę trzecią[5], że wykazano zgodność z kryteriami certyfikacji;

15. *podmiot certyfikujący* oznacza będący stroną trzecią[6]podmiot oceniający zgodność[7], posługujący się mechanizmami certyfikacji[8];

16. *system certyfikacji* oznacza system certyfikacji dotyczący określonych produktów, procesów i usług, względem których stosuje się te same określone wymogi, szczególne zasady i procedury[9];

17. *kryteria* lub kryteria certyfikacji oznaczają kryteria, na podstawie których dokonuje się certyfikacji (oceny zgodności)[10];

18. *krajowa jednostka akredytująca* oznacza jedyną autorytatywną jednostkę w państwie członkowskim, wyznaczoną zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008, udzielającą akredytacji na podstawie upoważnienia udzielonego jej przez państwo[11].

---

zgodnie z którymi jedna organizacja jest właścicielem systemu, inna zaś (lub kilka innych organizacji) dokonuje oceny.

[4] Artykuł 43 ust. 1, 3 i 6.

[5] Należy zauważyć, że zgodnie z ISO 17000 atestację (certyfikację) przez stronę trzecią „stosuje się względem wszystkich przedmiotów oceny zgodności" (5.5) „z wyjątkiem samych jednostek oceniających zgodność, względem których stosuje się akredytację" (5.6).

[6] Ocenę zgodności dokonywaną przez stronę trzecią przeprowadza organizacja, która jest niezależna od osoby lub organizacji zapewniającej jej przedmiot lub jest niezależna od interesów użytkownika tego przedmiotu, por. ISO 17000, 2.4.

[7] Zobacz ISO 17000, 2.5: „podmiot świadczący usługi oceny zgodności"; ISO 17011: „podmiot świadczący usługi oceny zgodności, który może być przedmiotem akredytacji"; ISO 17065, 3.12.

[8] Artykuł 42 ust. 1 i 5 RODO.

[9] Zobacz pkt 3.9 w związku z załącznikiem B do ISO 17065.

[10] Zobacz art. 42 ust. 5.

[11] Zobacz art. 2 pkt 11 rozporządzenia (WE) nr 765/2008.

3 INTERPRETACJA „AKREDYTACJI” DLA CELÓW ART. 43 RODO

19. W RODO nie uwzględniono definicji akredytacji. W art. 2 pkt 10 rozporządzenia (WE) nr 765/2008, które ustanawia ogólne wymagania w zakresie akredytacji, zdefiniowano akredytację jako

20. „poświadczenie przez krajową jednostkę akredytującą, że jednostka oceniająca zgodność spełnia wymagania określone w normach zharmonizowanych oraz – w stosownych przypadkach – wszelkie dodatkowe wymagania, w tym wymagania określone w odpowiednich systemach sektorowych konieczne do realizacji określonych czynności związanych z oceną zgodności”.

21. Zgodnie z ISO/IEC 17011

22. „akredytacja to atestacja przez stronę trzecią, dotycząca jednostki oceniającej zgodność, służąca formalnemu wykazaniu jej kompetencji do wykonywania określonych zadań w zakresie oceny zgodności”.

23. Artykuł 43 ust. 1 stanowi:

24. „Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 57 i 58 podmiot certyfikujący, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie ochrony danych dokonuje certyfikacji i jej przedłużenia po poinformowaniu organu nadzorczego w celu umożliwienia mu w razie potrzeby wykonywania uprawnień na mocy art. 58 ust. 2 lit. h). Państwa członkowskie zapewniają akredytację tych podmiotów certyfikujących przez:

    a) organ nadzorczy właściwy zgodnie z art. 55 lub 56; lub
    b) krajową jednostkę akredytującą określoną zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 – zgodnie z EN-ISO/IEC 17065/2012 – oraz zgodnie z dodatkowymi wymogami określonymi przez organ nadzorczy właściwy zgodnie z. 55 lub 56”.

25. W odniesieniu do RODO wymogi w zakresie akredytacji będą zgodne z:

- ISO/IEC 17065/2012 i dodatkowymi wymogami ustanowionymi przez organ nadzorczy właściwy zgodnie z art. 43 ust. 1 lit. b), gdy akredytacji dokonuje krajowa jednostka akredytująca, oraz przez organ nadzorczy, gdy sam dokonuje akredytacji.

26. W obu przypadkach ujednolicone wymogi muszą obejmować wymogi, o których mowa w art. 43 ust. 2.

27. Europejska Rada Ochrony Danych przyznaje, że celem akredytacji jest zapewnienie autorytatywnego potwierdzenia kompetencji jednostki do wykonywania certyfikacji (działalności z zakresu oceny zgodności)[12]. W kontekście RODO akredytację rozumie się w następujący sposób:

[12] Porównaj motyw 15 rozporządzenia (WE) nr 765/2008.

28. poświadczenie[13] przez krajową jednostkę akredytującą lub organ nadzorczy, że podmiot certyfikujący[14] posiada kwalifikacje, aby dokonywać certyfikacji na podstawie art. 42 i 43 RODO, uwzględniając ISO/IEC 17065/2012 i dodatkowe wymogi ustanowione przez organ nadzorczy lub przez Radę.

4 AKREDYTACJA ZGODNIE Z ART. 43 UST. 1 RODO

29. W art. 43 ust. 1 uznaje się, że istnieje kilka możliwości dotyczących akredytacji podmiotów certyfikujących. W RODO wymaga się od organów nadzorczych i od państw członkowskich, aby zdefiniowały proces akredytacji podmiotów certyfikujących. W niniejszej sekcji określono dostępne sposoby akredytacji określone w art. 43.

4.1 Rola państw członkowskich

30. W art. 43 ust. 1 wymaga się od państw członkowskich *zapewnienia* akredytacji podmiotów certyfikujących, pozwala się jednak każdemu państwu członkowskiemu na określenie kto powinien być odpowiedzialny za dokonywanie oceny prowadzącej do akredytacji. Na podstawie art. 43 ust. 1 dostępne są trzy możliwości; akredytacji dokonuje:

1) wyłącznie organ nadzorczy na podstawie własnych wymogów;
2) wyłącznie krajowa jednostka akredytująca określona zgodnie z rozporządzeniem (WE) nr 765/2008 i na podstawie ISO/IEC 17065/2012 oraz zgodnie z dodatkowymi wymogami określonymi przez właściwy organ nadzorczy; lub
3) zarówno organ nadzorczy, jak i krajowa jednostka akredytująca (zgodnie z wszystkimi wymogami wymienionymi w pkt 2 powyżej).

31. Dane państwo członkowskie decyduje, czy czynności związanych z akredytacją dokona krajowa jednostka akredytująca, organ nadzorczy, czy oba te podmioty, w każdym wypadku powinno ono jednak zapewnić udostępnienie odpowiednich zasobów[15].

4.2 Interakcja z rozporządzeniem (WE) nr 765/2008

32. Europejska Rada Ochrony Danych zauważa, że w art. 2 pkt 11 rozporządzenia (WE) nr 765/2008 zdefiniowano krajową jednostkę akredytującą jako *„jedyną autorytatywną* jednostkę w państwie członkowskim, udzielającą akredytacji na podstawie upoważnienia udzielonego jej przez państwo".

33. Artykuł 2 pkt 11 może być postrzegany jako niespójny z art. 43 ust. 1 RODO, w którym zezwala się na akredytację przez inny podmiot niż krajowa jednostka akredytująca państwa członkowskiego. Europejska Rada Ochrony Danych uważa, że prawodawstwo UE ma na celu odstąpienie od ogólnej zasady, zgodnie z którą akredytacji może dokonać wyłącznie krajowa jednostka akredytująca, udzielając organom nadzorczym takiego samego uprawnienia dotyczącego akredytacji podmiotów certyfikujących. Artykuł 43 ust. 1 stanowi zatem *lex specialis* względem art. 2 pkt 11 rozporządzenia 765/2008.

---

[13] Porównaj art. 2 pkt 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu.
[14] Porównaj z definicją terminu „akredytacja" zgodnie z ISO 17011.
[15] Zobacz art. 4 ust. 9 rozporządzenia (WE) nr 765/2008.

4.3 Rola krajowej jednostki akredytującej

34. Artykuł 43 ust. 1 lit. b) stanowi, że krajowa jednostka akredytująca będzie dokonywała akredytacji podmiotów certyfikujących zgodnie z ISO/IEC 17065/2012 oraz zgodnie z dodatkowymi wymogami określonymi przez właściwy organ nadzorczy.

35. Dla zachowania jasności Europejska Rada Ochrony Danych zauważa, że szczególne odniesienie w art. 43 ust. 3 do „ust. 1 lit. [b])" oznacza, że zwrot „wymogi te" odnosi się do „dodatkowych wymogów" ustanowionych przez właściwy organ nadzorczy na podstawie art. 43 ust. 1 lit. b) oraz wymogów określonych w art. 43 ust. 2.

36. W procesie akredytacji krajowe jednostki akredytujące stosują dodatkowe wymogi, które mają dostarczyć organy nadzorcze.

37. Podmiot certyfikujący posiadający akredytację na podstawie ISO/IEC 17065/2012 w odniesieniu do systemów certyfikacji innych niż związane z RODO, który chce rozszerzyć zakres swojej akredytacji tak, aby obejmowała ona certyfikację wydaną zgodnie z RODO, będzie musiał spełnić dodatkowe wymogi ustanowione przez organ nadzorczy, jeżeli akredytacji dokonuje krajowa jednostka akredytująca. Jeżeli akredytację na potrzeby certyfikacji na podstawie RODO oferuje tylko właściwy organ nadzorczy, podmiot certyfikujący wnioskujący o akredytację będzie musiał spełnić wymogi określone przez odpowiedni organ nadzorczy.

4.4 Rola organu nadzorczego

38. Europejska Rada Ochrony Danych zauważa, że art. 57 ust. 1 lit. q) stanowi, że organ nadzorczy akredytuje podmiot certyfikujący na mocy art. 43 w ramach zadań organu nadzorczego zgodnych z art. 57, a art. 58 ust. 3 lit. e) stanowi, że organowi nadzorczemu przysługują uprawnienia w zakresie wydawania zezwoleń i uprawnienia doradcze w postaci akredytowania na mocy art. 43 podmiotów certyfikujących. Sformułowanie art. 43 ust. 1 zapewnia pewien stopień elastyczności a funkcję akredytującą organu nadzorczego należy postrzegać jak zadanie tylko w stosownych przypadkach. Do celów uściślenia tej kwestii można wykorzystać prawo państwa członkowskiego. W procesie akredytacji dokonywanej przez krajową jednostkę akredytującą wymaga się jednak od podmiotu certyfikującego zgodnie z art. 43 ust. 2 lit. a), aby w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie oferowanego przez nią mechanizmu certyfikacji[16].

39. Jeżeli państwo członkowskie zastrzega sobie, że podmioty certyfikujące mają być akredytowane przez organ nadzorczy, organ ten powinien ustanowić wymogi w zakresie akredytacji obejmujące wymogi wyszczególnione w art. 43 ust. 2, lecz nie ograniczające się do nich. W porównaniu z obowiązkami związanymi z akredytacją podmiotów certyfikujących przez krajowe jednostki certyfikujące, w art. 43 przewidziano mniej instrukcji dotyczących wymogów w zakresie akredytacji w przypadku, gdy dokonuje jej sam organ nadzorczy. W celu przyczynienia się do jednolitego podejścia do akredytacji kryteria akredytacji stosowane przez organ nadzorczy należy oprzeć na ISO/IEC 17065 oraz uzupełnić je dodatkowymi wymogami, które organ nadzorczy ustanawia na podstawie art. 43 ust. 1 lit. b).

[16] W dodatkowych wymogach ustanowionych przez organ nadzorczy zgodnie z art. 43 ust. 1 lit. b) należy określić wymogi dotyczące niezależności i wiedzy fachowej. Zobacz również załącznik 1 do wytycznych.

Europejska Rada Ochrony Danych zauważa, że art. 43 ust. 2 lit. a)–e) odzwierciedlają i uszczegóławiają wymogi ISO 17065, co przyczyni się do zachowania spójności.

40. Jeżeli państwo członkowskie zastrzega sobie, że podmioty certyfikujące mają być akredytowane przez krajowe jednostki akredytujące, organ nadzorczy powinien ustanowić dodatkowe wymogi uzupełniające istniejące praktyki przewidziane w rozporządzeniu (WE) nr 765/2008 (w którym art. 3–14 odnoszą się do organizacji i dokonywania akredytacji jednostek oceniających zgodność) oraz przepisy techniczne określające metody i procedury organów nadzorczych. W tym świetle w rozporządzeniu (WE) nr 765/2008 przewidziano dalsze wytyczne: w art. 2 pkt 10 zdefiniowano akredytację i odniesiono się do „zharmonizowanych norm" i „wszelkich dodatkowych wymagań, w tym wymagań określonych w odpowiednich systemach sektorowych". Wynika z tego, że dodatkowe wymogi ustanowione przez organ nadzorczy powinny obejmować szczególne wymogi i koncentrować się na ułatwieniu m.in. oceny niezależności i poziomu wiedzy fachowej w zakresie ochrony danych osobowych podmiotów certyfikujących, np. ich zdolności do oceny i certyfikacji operacji przetwarzania danych osobowych przez administratorów i podmioty przetwarzające na podstawie art. 42 ust. 1. Obejmują one kompetencje wymagane w odniesieniu do systemów sektorowych i ochrony podstawowych praw i wolności osób fizycznych, a w szczególności ich prawa do ochrony danych osobowych[17]. Załącznik do niniejszych wytycznych może być pomocny w dostarczeniu właściwym organom nadzorczym informacji niezbędnych przy ustanawianiu dodatkowych wymogów zgodnie z art. 43 ust. 1 lit. b) i art. 43 ust. 3.

41. Artykuł 43 ust. 6 stanowi, że „[o]rgan nadzorczy w łatwo dostępny sposób podaje do wiadomości publicznej wymogi, o których mowa w ust. 3 niniejszego artykułu, oraz kryteria, o których mowa w art. 42 ust. 5". W związku z tym, aby zapewnić przejrzystość, należy publikować wszystkie kryteria i wymogi zatwierdzone przez organ nadzorczy. Jeżeli chodzi o jakość i zaufanie względem podmiotów certyfikujących, byłoby pożądane, aby wszelkie wymogi dotyczące akredytacji były łatwo dostępne publicznie.

4.5 Organ nadzorczy działający w charakterze podmiotu certyfikującego

42. Artykuł 42 ust. 5 stanowi, że organ nadzorczy może dokonać certyfikacji, zgodnie z RODO nie musi być on jednak akredytowany, aby spełniał wymogi rozporządzenia (WE) nr 765/2008. Europejska Rada Ochrony Danych zauważa, że w art. 43 ust. 1 lit. a) i szczególnie w art. 58 ust. 2 lit. h), art. 58 ust. 3 lit. a), e)–f) nadaje się organom nadzorczym uprawnienia do dokonywania zarówno akredytacji, jak i certyfikacji, i jednocześnie do udzielania porad i w stosownych przypadkach cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu nieudzielania certyfikacji.

43. Mogą wystąpić sytuacje, w których stosowne lub wymagane jest rozdzielenie ról i obowiązków związanych z akredytacją i certyfikacją, np. jeżeli w państwie członkowskim współistnieją organ nadzorczy i inne podmioty certyfikujące i dokonują one certyfikacji w tym samym zakresie. Organy nadzorcze powinny zatem podjąć wystarczające działania organizacyjne, aby rozdzielić zadania na podstawie RODO w celu osadzenia i ułatwienia mechanizmów certyfikacji, przy jednoczesnym podjęciu środków ostrożności, aby uniknąć konfliktów interesów, które mogą wynikać z tych zadań. Ponadto państwa członkowskie

[17] Artykuł 1 ust. 2 RODO.

i organy nadzorcze, opracowując krajowe prawo i procedury związane z akredytacją i certyfikacją zgodnie z RODO, powinny mieć na uwadze jednolity poziom europejski.

4.6 Wymogi w zakresie akredytacji

44. W załączniku do niniejszych wytycznych przedstawiono wskazówki dotyczące sposobu określenia dodatkowych wymogów w zakresie akredytacji. Określono w nim stosowne przepisy ujęte w RODO i zasugerowano wymogi, które organy nadzorcze i krajowe jednostki akredytujące powinny uwzględnić, aby zapewnić zgodność z przepisami RODO.

45. Jak ustalono powyżej, jeżeli podmioty certyfikujące są akredytowane przez krajową jednostkę akredytującą na podstawie rozporządzenia (WE) nr 765/2008, odpowiednią normą w zakresie akredytacji będzie ISO/IEC 17065/2012 uzupełniona dodatkowymi wymogami ustanowionymi przez organ nadzorczy. W świetle ochrony praw podstawowych na podstawie RODO, art. 43 ust. 2 odzwierciedla ogólne przepisy ISO/IEC 17065/2012. W ramach ujętych w załączniku zastosowano art. 43 ust. 2 i ISO/IEC 17065/2012 jako podstawę określenia wymogów i dodatkowych kryteriów związanych z oceną wiedzy fachowej podmiotów certyfikujących w zakresie ochrony danych oraz ich zdolności do poszanowania praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych, jak zagwarantowano w RODO. Europejska Rada Ochrony Danych zauważa, że koncentrują się one w szczególności na zapewnieniu, aby podmioty certyfikujące miały odpowiedni poziom wiedzy fachowej w zakresie ochrony danych zgodnie z art. 43 ust. 1.

46. Dodatkowe wymogi w zakresie akredytacji ustanowione przez organ nadzorczy będą miały zastosowanie względem wszystkich podmiotów certyfikujących zwracających się o akredytację. Jednostka akredytująca oceni, czy podmiot certyfikujący jest właściwy do dokonywania certyfikacji zgodnie z dodatkowymi wymogami i przedmiotem certyfikacji. Należy uwzględnić odniesienia do konkretnych sektorów lub obszarów certyfikacji, do których podmiot certyfikujący posiada akredytację.

47. Europejska Rada Ochrony Danych zauważa również, że w przypadku gdy inne podmioty zewnętrzne, takie jak laboratoria lub audytorzy, wykonują część elementów czynności w zakresie certyfikacji w imieniu akredytowanego podmiotu certyfikującego, poza wymogami ujętymi w ISO/IEC 17065/2012 wymagana jest również szczególna wiedza fachowa w dziedzinie ochrony danych. W takich przypadkach nie jest możliwa akredytacja takich zewnętrznych podmiotów na podstawie samego RODO. Aby zapewnić jednak odpowiednie kwalifikacje takich podmiotów do wykonywania ich działań w imieniu akredytowanych podmiotów certyfikujących, konieczne jest zapewnienie przez akredytowany podmiot certyfikujący, aby podmiot zewnętrzny również posiadał wiedzę fachową z zakresu ochrony danych wymaganą od podmiotów akredytowanych i wykazał się taką wiedzą, w odniesieniu do stosownego wykonywanego działania.

48. Ramy służące określeniu dodatkowych wymogów w zakresie akredytacji przedstawione w załączniku do niniejszych wytycznych nie są podręcznikiem procedur dotyczących procesu akredytacji dokonywanej przez krajową jednostkę akredytującą lub organ nadzorczy. Zawiera on wskazówki dotyczące struktury i metodyki, jest zatem zestawem narzędzi dla organów nadzorczych pomocnym w określeniu dodatkowych wymogów w zakresie akredytacji.

ZAŁĄCZNIK 1

Załącznik 1 zawiera wytyczne dotyczące określenia dodatkowych wymogów akredytacyjnych w odniesieniu do normy ISO/IEC 17065/2012, zgodnie z art. 43 ust. 1 lit. b) i art. 43 ust. 3 RODO.

W załączniku przedstawiono proponowane wymogi, które opracowuje organ nadzorczy ds. ochrony danych i które mają zastosowanie podczas akredytacji podmiotu certyfikującego przez krajową jednostkę akredytującą lub właściwy organ nadzorczy[18]. Te dodatkowe wymogi należy zgłosić Europejskiej Radzie Ochrony Danych przed ich zatwierdzeniem na podstawie art. 64 ust. 1 lit. c).

Niniejszy załącznik należy interpretować w powiązaniu z normą ISO/IEC 17065/2012. Stosowane tu numery sekcji odpowiadają numerom stosowanym w normie ISO/IEC 17065/2012. Dobrą praktyką byłoby stosowanie tego podejścia przez organy nadzorcze w ramach procedury akredytacji zgodnie z art. 43 ust. 1 lit. a), o ile jest to wykonalne. Ułatwi to akredytację zharmonizowaną na szczeblu UE.

Niezależnie od poniższych wytycznych lub braku wytycznych dotyczących jakiegokolwiek punktu normy ISO/IEC 17065/2012 właściwy organ nadzorczy może sformułować dalsze dodatkowe wymogi dotyczące tych punktów, pod warunkiem zgodności z prawem krajowym.

0 WSTĘP

[W niniejszej sekcji ujmuje się wszelkie ewentualne uzgodnione warunki współpracy między krajową jednostką akredytującą a organem nadzorczym ds. ochrony danych, np. określające, kto powinien odpowiadać za przyjmowanie wniosków lub jak zorganizować uznawanie zatwierdzonych kryteriów w ramach procesu akredytacji.]

1 ZAKRES[19]

Zakres normy ISO/IEC 17065/2012 stosuje się zgodnie z RODO. Dalsze informacje znajdują się w wytycznych w sprawie akredytacji i certyfikacji. Podczas procesu akredytacji krajowa jednostka akredytująca i właściwy organ nadzorczy powinny w swojej ocenie uwzględniać zakres mechanizmu certyfikacji (na przykład certyfikacja operacji przetwarzania w chmurze), w szczególności w odniesieniu do kryteriów, wiedzy fachowej i metodyki oceny. Szeroki zakres normy ISO/IEC 17065/2012, obejmujący produkty, procesy i usługi, nie powinien prowadzić do zaniżania ani zastępowania wymogów RODO. Na przykład mechanizm zarządzania nie może być jedynym elementem mechanizmu certyfikacji, ponieważ certyfikacja musi obejmować operacje przetwarzania danych osobowych. Zgodnie z art. 42 ust. 1 RODO certyfikacja ma zastosowanie wyłącznie do operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające.

2 ODNIESIENIE NORMATYWNE

Przepisy RODO są nadrzędne wobec normy ISO/IEC 17065/2012. Jeżeli w wymogach dodatkowych lub w mechanizmie certyfikacji znajduje się odniesienie do innych norm ISO, należy je interpretować zgodnie z wymogami określonymi w RODO.

---

[18] Informacje na temat procesu zatwierdzania kryteriów certyfikacji znajdują się w sekcji 4 wytycznych dotyczących certyfikacji.

[19] Numeracja odpowiada normie ISO/IEC 17065/2012.

3 TERMINY I DEFINICJE

W kontekście niniejszego załącznika stosuje się terminy i definicje zawarte w wytycznych dotyczących akredytacji (WP 261) i certyfikacji (EROD 1/2018) i są one nadrzędne wobec definicji ISO.

4 OGÓLNE WYMOGI W ZAKRESIE AKREDYTACJI

4.1 Kwestie prawne i umowne

4.1.1 Odpowiedzialność prawna

Podmiot certyfikujący powinien zawsze być w stanie wykazać krajowej jednostce akredytującej lub właściwemu organowi nadzorczemu, że posiada aktualne procedury potwierdzające przestrzeganie obowiązków prawnych określonych w warunkach akredytacji, w tym dodatkowych wymogów dotyczących stosowania rozporządzenia (UE) 2016/679. Należy zauważyć, że ponieważ podmiot certyfikujący sam również jest administratorem lub podmiotem przetwarzającym dane, musi on być w stanie wykazać posiadanie procedur i środków zgodnych z rozporządzeniem (UE) 2016/679, szczególnie w odniesieniu do administrowania danymi osobowymi organizacji będącej klientem i ich obsługi w procesie certyfikacji.

Właściwy organ nadzorczy może dodać dalsze wymogi i procedury w celu sprawdzenia zgodności podmiotów certyfikujących z RODO przed akredytacją.

4.1.2 Umowa o certyfikacji

Minimalne wymogi dotyczące umowy o certyfikacji uzupełnia się o następujące punkty:

Podmiot certyfikujący musi wykazać, że jego umowy o certyfikacji, oprócz spełniania wymogów zawartych w normie ISO/IEC 17065/2012:

1. zobowiązują wnioskodawcę do stałego spełniania zarówno ogólnych wymogów w zakresie certyfikacji w rozumieniu pkt 4.1.2.2 lit. a) normy ISO/IEC 17065/2012, jak kryteriów zatwierdzonych przez właściwy organ nadzorczy lub EROD zgodnie z art. 43 ust. 2 lit. b) i art. 42 ust. 5;
2. zobowiązują wnioskodawcę, aby zapewnił pełną przejrzystość wobec właściwego organu nadzorczego w odniesieniu do procedury certyfikacji, w tym kwestii objętych postanowieniami umownymi o poufności, dotyczących ochrony danych, zgodnie z art. 42 ust. 7 i art. 58 ust. 1 lit. c);
3. nie ograniczają odpowiedzialności wnioskodawcy za zgodność z rozporządzeniem (UE) 2016/679 i pozostają bez uszczerbku dla zadań i uprawnień organów nadzorczych, które są właściwe na mocy art. 42 ust. 5;
4. zobowiązują wnioskodawcę do dostarczenia podmiotowi certyfikującemu wszelkich informacji i dostępu do prowadzonych przez wnioskodawcę czynności przetwarzania w zakresie niezbędnym do przeprowadzenia procedury certyfikacji zgodnie z art. 42 ust. 6;
5. zobowiązują wnioskodawcę do przestrzegania obowiązujących terminów i procedur, np. wynikających z programu certyfikacji lub innych przepisów;
6. w odniesieniu do pkt 4.1.2.2 lit. c) ppkt 1) normy ISO/IEC 17065/2012 – określają zasady ważności, przedłużenia i cofnięcia certyfikacji zgodnie z art. 42 ust. 7 i art. 43 ust. 4, w tym zasady określające odpowiednie odstępy czasu na ponowną ocenę lub przegląd (regularność) zgodnie z art. 42 ust. 7;

7. zezwalają podmiotowi certyfikującemu na ujawnienie wszelkich informacji niezbędnych do przyznania certyfikacji zgodnie z art. 42 ust. 8 i art. 43 ust. 5;
8. zawierają przepisy dotyczące niezbędnych środków ostrożności w odniesieniu do rozpatrywania skarg w rozumieniu pkt 4.1.2.2 lit. c) ppkt 2), a ponadto (lit. j)) zawierają również wyraźne oświadczenia na temat struktury i procedury rozpatrywania skarg zgodnie z art. 43 ust. 2 lit. d);
9. w uzupełnieniu minimalnych wymogów, o których mowa w pkt 4.1.2.2 normy ISO/IEC 17065/2012, w przypadku gdy skutki cofnięcia lub zawieszenia akredytacji dla podmiotu certyfikującego mają konsekwencje dla klienta, należy je również uwzględnić;
10. zobowiązują wnioskodawcę do powiadomienia podmiotu certyfikującego o ewentualnych istotnych zmianach jego sytuacji faktycznej lub prawnej oraz o zmianach produktów, procesów i usług objętych certyfikacją.

4.1.3 Stosowanie znaków jakości i oznaczeń w dziedzinie ochrony danych

Certyfikaty, znaki jakości i oznaczenia stosuje się wyłącznie w sposób zgodny z art. 42 i 43 oraz z wytycznymi w sprawie akredytacji i certyfikacji.

4.2 Zarządzanie bezstronnością

Jednostka akredytująca zapewnia, że w uzupełnieniu do wymogu określonego w sekcji 4.2 normy ISO/IEC 17065/2012:

1. jednostka certyfikująca spełnia dodatkowe wymogi określone przez właściwy organ nadzorczy (na podstawie art. 43 ust. 1 lit. b)),
    a. zgodnie z art. 43 ust. 2 lit. a) przedstawia odrębne dowody swojej niezależności, w szczególności w odniesieniu do finansowania podmiotu certyfikującego w zakresie, w jakim wiąże się to z zapewnieniem bezstronności;
    b. jej zadania i obowiązki nie prowadzą do konfliktu interesów zgodnie z art. 43 ust. 2 lit. e);
2. jednostka certyfikująca nie jest powiązana w istotny sposób z klientem, którego ocenia.

4.3 Odpowiedzialność i finansowanie

W uzupełnieniu do wymogu zawartego w pkt 4.3.1 normy ISO/IEC 17065/2012 jednostka akredytująca regularnie zapewnia, że podmiot certyfikujący posiada odpowiednie środki (np. ubezpieczenia lub rezerwy) w celu pokrycia swoich zobowiązań w regionach geograficznych, w których prowadzi działalność.

4.4 Niedyskryminujące warunki

Organ nadzorczy może sformułować dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

4.5 Poufność

Organ nadzorczy może sformułować dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

4.6 Informacje dostępne publicznie

Jednostka akredytująca, w uzupełnieniu do wymogu określonego w pkt 4.6. normy ISO/IEC 17065/2012, zobowiązuje podmiot certyfikujący co najmniej do tego, aby:

1. wszystkie (obecne i poprzednie) wersje zatwierdzonych kryteriów stosowanych w rozumieniu art. 42 ust. 5, jak również wszystkie procedury certyfikacji były

opublikowane i łatwo dostępne publicznie, zasadniczo wraz z określeniem terminu ważności;

2. informacje na temat procedur rozpatrywania skarg i odwołań były podane do wiadomości publicznej zgodnie z art. 43 ust. 2 lit. d).

5 WYMOGI STRUKTURALNE, ART. 43 UST. 4 [„WŁAŚCIWA" OCENA]

5.1 Struktura organizacyjna i ścisłe kierownictwo

Organ nadzorczy może sformułować dodatkowe wymogi.

5.2 Mechanizmy zapewnienia bezstronności

Organ nadzorczy może sformułować dodatkowe wymogi.

6 WYMOGI DOTYCZĄCE ZASOBÓW

6.1 Personel podmiotu certyfikującego

Jednostka akredytująca, w uzupełnieniu do wymogu określonego w sekcji 6 normy ISO/IEC 17065/2012, zapewnia w odniesieniu do każdego podmiotu certyfikującego, że jego personel:

1. wykazał posiadanie odpowiedniej i aktualnej wiedzy i doświadczenia w zakresie ochrony danych zgodnie z art. 43 ust. 1;
2. charakteryzuje się niezależnością i dysponuje aktualną wiedzą fachową w odniesieniu do przedmiotu certyfikacji zgodnie z art. 43 ust. 2 lit. a) i nie jest w sytuacji konfliktu interesów zgodnie z art. 43 ust. 2 lit. e);
3. zobowiązuje się do przestrzegania kryteriów, o których mowa w art. 42 ust. 5, zgodnie z art. 43 ust. 2 lit. b);
4. dysponuje odpowiednią wiedzą i doświadczeniem w zakresie stosowania przepisów dotyczących ochrony danych;
5. dysponuje odpowiednią wiedzą i doświadczeniem w zakresie technicznych i organizacyjnych środków ochrony danych;
6. jest w stanie wykazać się doświadczeniem w dziedzinach wymienionych w dodatkowych wymaganiach 6.1.1, 6.1.4 i 6.1.5, a konkretnie:

pracownicy posiadający fachową wiedzę techniczną:

- posiadają kwalifikacje w odpowiedniej dziedzinie technicznej, odpowiadające co najmniej poziomowi 6 według europejskich ram kwalifikacji[20], lub uznany chroniony tytuł (np. dyplom inżynierski) w odpowiednim zawodzie regulowanym lub posiadają znaczące doświadczenie zawodowe;
- *pracownicy odpowiedzialni za decyzje w sprawie certyfikacji* muszą posiadać istotne doświadczenie zawodowe w zakresie określania i wdrażania środków ochrony danych;
- *pracownicy odpowiedzialni za ocenę* muszą posiadać doświadczenie zawodowe w zakresie technicznych środków ochrony danych oraz wiedzę i doświadczenie

[20] Zob. narzędzie do porównania ram kwalifikacji na stronie https://ec.europa.eu/ploteus/en/compare?

w zakresie porównywalnych procedur (np. certyfikacji/audytów), a w stosownych przypadkach wykazać rejestrację;

pracownicy muszą wykazać, że utrzymują wiedzę specjalistyczną w zakresie umiejętności technicznych i audytowych poprzez ustawiczne doskonalenie zawodowe;

pracownicy posiadający fachową wiedzę prawniczą:

- mają ukończone studia prawnicze na uczelni uznanej na szczeblu unijnym lub krajowym, trwające co najmniej osiem semestrów i zakończone uzyskaniem stopnia magistra prawa lub równoważnego stopnia bądź posiadają znaczące doświadczenie zawodowe;
- *pracownicy odpowiedzialni za decyzje w sprawie certyfikacji* muszą wykazać się znaczącym doświadczeniem zawodowym w zakresie prawa ochrony danych i być zarejestrowani zgodnie z wymogami państwa członkowskiego;
- *pracownicy odpowiedzialni za ocenę* muszą wykazać posiadanie co najmniej dwuletniego doświadczenia zawodowego w zakresie prawa ochrony danych oraz wiedzy i doświadczenia w zakresie porównywalnych procedur (np. certyfikacji/audytów), oraz być zarejestrowani, o ile jest to wymagane przez dane państwo członkowskie;
    - pracownicy muszą wykazać, że utrzymują wiedzę specjalistyczną w zakresie umiejętności technicznych i audytowych poprzez ustawiczne doskonalenie zawodowe.

6.2 Zasoby na potrzeby oceny

Organ nadzorczy może sformułować dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

7 WYMOGI DOTYCZĄCE PROCESÓW, ART. 43 UST. 2 LIT. C) I D)

7.1 Wytyczne ogólne

Jednostka akredytująca, w uzupełnieniu do wymogu określonego w sekcji 7.1 normy ISO/IEC 17065/2012, jest zobowiązana zapewnić, że:

1. podmioty certyfikujące spełniają dodatkowe wymogi właściwego organu nadzorczego (zgodnie z art. 43 ust. 1 lit. b)) przy składaniu wniosku, tak aby zadania i obowiązki nie prowadziły do powstania konfliktu interesów zgodnie z art. 43 ust. 2 lit. b);
2. powiadamiają właściwe organy nadzorcze, zanim jednostka certyfikująca zacznie działać w oparciu o zatwierdzony europejski znak jakości ochrony danych w nowym państwie członkowskim za pośrednictwem biura pomocniczego.

7.2 Wniosek

W uzupełnieniu do pkt 7.2 normy ISO/IEC 17065/2012 należy wymagać, aby:

1. przedmiot certyfikacji (przedmiot oceny) był szczegółowo opisany we wniosku wraz z interfejsami i transferami do innych systemów i organizacji, protokołów i innych gwarancji;
2. we wniosku określono, czy korzysta się z podmiotów przetwarzających, a jeżeli wnioskodawcą jest podmiot przetwarzający – aby opisano jego obowiązki i zadania oraz dołączono odnośną umowę z administratorem lub podmiotem przetwarzającym.

7.3 Rozpatrywanie wniosków

W uzupełnieniu do pkt 7.3 normy ISO/IEC 17065/2012 należy wymagać, aby:

1. w umowie o certyfikacji określone były wiążące metody oceny w odniesieniu do przedmiotu oceny;
2. w ocenie dotyczącej wystarczającej wiedzy fachowej, przewidzianej w pkt 7.3 lit. e), uwzględniano w odpowiednim zakresie zarówno techniczną, jak i prawną wiedzę fachową w zakresie ochrony danych.

7.4 Ocena

W uzupełnieniu do pkt 7.4 normy ISO/IEC 17065/2012 w mechanizmach certyfikacji należy określić wystarczające metody oceny zgodności operacji przetwarzania z kryteriami certyfikacji, w tym na przykład, w stosownych przypadkach:

1. metodę oceny konieczności i proporcjonalności operacji przetwarzania w odniesieniu do ich celu oraz osób, których dane dotyczą;
2. metodę oceny zakresu, składu i analizy wszelkiego ryzyka uwzględnionego przez administratora i podmiot przetwarzający w odniesieniu do skutków prawnych zgodnie z art. 30, 32, 35 i 36 RODO oraz w odniesieniu do definicji środków technicznych i organizacyjnych zgodnie z art. 24, 25 i 32 RODO w zakresie, w jakim wyżej wymienione artykuły mają zastosowanie do przedmiotu certyfikacji;
3. metodę oceny środków zaradczych, w tym gwarancji, zabezpieczeń i procedur służących zapewnieniu ochrony danych osobowych w kontekście operacji przetwarzania, które mają być przypisane do przedmiotu certyfikacji, oraz służących wykazaniu, że spełnione są wymogi prawne określone w kryteriach oraz
4. sposób dokumentowania metod i ustaleń.

Podmiot certyfikujący powinien być zobowiązany do zapewnienia standaryzacji i ogólnego stosowania tych metod oceny. Oznacza to stosowanie porównywalnych metod oceny do porównywalnych przedmiotów oceny. Wszelkie odstępstwa od tej procedury muszą być uzasadnione przez podmiot certyfikujący.

W uzupełnieniu do pkt 7.4.2 normy ISO/IEC 17065/2012 należy zezwolić na przeprowadzanie oceny przez ekspertów zewnętrznych uznanych przez jednostkę certyfikującą.

W uzupełnieniu do pkt 7.4.5 normy ISO/IEC 17065/2012 należy wymagać, aby certyfikacja w zakresie ochrony danych zgodna z art. 42 i 43 RODO, która obejmuje już część przedmiotu certyfikacji, mogła być włączona do bieżącej procedury certyfikacji. Nie będzie ona jednak wystarczająca do całkowitego zastąpienia (częściowych) ocen. Podmiot certyfikujący powinien być zobowiązany do sprawdzenia zgodności z kryteriami. Na potrzeby uznania należy w każdym wypadku wymagać dostępności pełnego sprawozdania z oceny lub informacji umożliwiających ocenę poprzedniej działalności w zakresie certyfikacji i jej wyników. Oświadczenie certyfikacyjne lub podobne świadectwa certyfikacji nie powinny być uznawane za wystarczające do zastąpienia sprawozdania.

W uzupełnieniu do pkt 7.4.6 normy ISO/IEC 17065/2012 należy zobowiązać podmiot certyfikujący, aby określił szczegółowo w swoim mechanizmie certyfikacji, w jaki sposób informacje wymagane w pkt 7.4.6 pozwalają klientowi (podmiotowi wnioskującemu o certyfikację) uzyskać wiedzę o niezgodnościach w odniesieniu do mechanizmu certyfikacji. W tym kontekście należy określić przynajmniej charakter i ramy czasowe takich informacji.

W uzupełnieniu do pkt 7.4.9 normy ISO/IEC 17065/2012 należy wymagać zapewnienia organowi nadzorczemu ds. ochrony danych pełnego dostępu do dokumentacji.

7.5 Przegląd

W uzupełnieniu do pkt 7.5 normy ISO/IEC 17065/2012 wymagane są procedury wydawania, regularnego przeglądu i cofania odpowiednich certyfikatów zgodnie z art. 43 ust. 2 i 3.

7.6 Decyzja o certyfikacji

W uzupełnieniu do pkt 7.6.1 normy ISO/IEC 17065/2012 podmiot certyfikujący powinien być zobowiązany do szczegółowego określenia w swoich procedurach, w jaki sposób zapewniona jest jego niezależność i odpowiedzialność w odniesieniu do poszczególnych decyzji o certyfikacji.

7.7 Dokumentacja certyfikacji

W uzupełnieniu do pkt 7.7.1 lit. e) normy ISO/IEC 17065/2012 i zgodnie z art. 42 ust. 7 RODO należy wymagać, aby okres ważności certyfikacji nie przekraczał trzech lat.

W uzupełnieniu do pkt 7.7.1 lit. e) normy ISO/IEC 17065/2012 należy wymagać, aby okres planowanego monitorowania w rozumieniu sekcji 7.9 również był dokumentowany.

W uzupełnieniu do pkt 7.7.1 lit. f) normy ISO/IEC 17065/2012 podmiot certyfikujący powinien być zobowiązany do określenia przedmiotu certyfikacji w dokumentacji certyfikacji (ze wskazaniem, w stosownych przypadkach, statusu wersji lub podobnych cech).

7.8 Wykaz certyfikowanych produktów

W uzupełnieniu do pkt 7.8 normy ISO/IEC 17065/2012 podmiot certyfikujący powinien być zobowiązany do przechowywania do wewnętrznego i publicznego wglądu informacji o certyfikowanych produktach, procesach i usługach. Podmiot certyfikujący podaje do wiadomości publicznej streszczenie sprawozdania z oceny, służące zapewnieniu przejrzystości co do przedmiotu certyfikacji i sposobu oceny. W streszczeniu przedstawia się między innymi:

a) zakres certyfikacji i miarodajny opis przedmiotu certyfikacji (przedmiotu oceny),

b) odpowiednie kryteria certyfikacji (z podaniem wersji lub statusu funkcjonalnego),

c) metody oceny i przeprowadzone badania,

d) wyniki.

W uzupełnieniu do pkt 7.8 normy ISO/IEC 17065/2012 i zgodnie z art. 43 ust. 5 RODO podmiot certyfikujący informuje właściwe organy nadzorcze o przyczynach udzielenia lub cofnięcia certyfikacji, o którą się do niego zwrócono.

7.9 Nadzór

W uzupełnieniu do pkt 7.9.1, 7.9.2 i 7.9.3 normy ISO/IEC 17065/2012 oraz zgodnie z art. 43 ust. 2 lit. c) RODO należy wprowadzić wymóg obowiązkowych regularnych środków monitorowania w celu utrzymania certyfikacji w okresie monitorowania.

7.10 Zmiany mające wpływ na certyfikację

W uzupełnieniu pkt 7.10.1 i 7.10.2 normy EN ISO/IEC 17065/2012 zmiany mające wpływ na certyfikację, które wymagają uwzględnienia przez jednostkę certyfikującą, obejmują: zmiany w przepisach prawnych dotyczących ochrony danych, przyjęcie aktów delegowanych Komisji Europejskiej zgodnie z art. 43 ust. 8 i 9, decyzje Europejskiej Rady Ochrony Danych oraz decyzje sądowe dotyczące ochrony danych. Zmiany proceduralne wymagające uwzględnienia mogą obejmować: okresy przejściowe, proces zatwierdzania przez właściwy organ nadzorczy, ponowną ocenę odnośnego przedmiotu certyfikacji oraz odpowiednie środki w celu cofnięcia certyfikacji, jeśli certyfikowana operacja przetwarzania danych nie jest już zgodna z aktualnymi kryteriami.

7.11 Wygaśnięcie, ograniczenie, zawieszenie lub cofnięcie certyfikacji

W uzupełnieniu do pkt 7.11.1 normy ISO/IEC 17065/2012 podmiot certyfikujący powinien być zobowiązany do niezwłocznego pisemnego powiadomienia właściwego organu nadzorczego oraz w stosownych przypadkach krajowej jednostki akredytującej o podjętych środkach oraz o kontynuacji, ograniczeniu, zawieszeniu lub cofnięciu certyfikacji.

Zgodnie z art. 58 ust. 2 lit. h) podmiot certyfikujący powinien być zobowiązany do przyjmowania od właściwego organu nadzorczego decyzji i zarządzeń o cofnięciu lub odmowie przyznania certyfikacji klientowi (wnioskodawcy), jeżeli wymóg certyfikacji nie został spełniony lub przestał być spełniany.

7.12 Ewidencja

Podmiot certyfikujący powinien być zobowiązany do przechowywania pełnej dokumentacji, która powinna być zrozumiała, aktualna i nadająca się do audytu.

7.13 Skargi i odwołania, art. 43 ust. 2 lit. d)

W uzupełnieniu do pkt 7.13.1 normy ISO/IEC 17065/2012 należy wymagać, aby podmiot certyfikujący określił:

a) kto może składać skargi lub zastrzeżenia,

b) kto rozpatruje skargi lub zastrzeżenia po stronie podmiotu certyfikującego,

c) jakie weryfikacje przeprowadza się w tym kontekście;

d) możliwości konsultacji z zainteresowanymi stronami.

W uzupełnieniu do pkt 7.13.2 normy ISO/IEC 17065/2012 należy wymagać, aby podmiot certyfikujący określił:

a) w jaki sposób i komu należy wydać potwierdzenie, o którym mowa,

b) terminy jego wydawania;

c) jakie procesy należy następnie uruchomić.

W uzupełnieniu do pkt 7.13.1 normy ISO/IEC 17065/2012 podmiot certyfikujący musi określić, w jaki sposób zapewniona jest odrębność rozpatrywania odwołań i skarg od czynności certyfikacyjnych.

8 WYMOGI DOTYCZĄCE SYSTEMU ZARZĄDZANIA

Zgodnie z ogólnym wymogiem dotyczącym systemu zarządzania przewidzianym w rozdziale 8 normy ISO/IEC 17065/2012 wdrażanie wszystkich wymogów zawartych w poprzednich rozdziałach w ramach stosowania mechanizmu certyfikacji przez akredytowany podmiot certyfikujący musi być dokumentowane, oceniane, kontrolowane i monitorowane w sposób niezależny

Podstawową zasadą zarządzania jest określenie systemu, w którym jego cele są ustalane skutecznie i efektywnie, co dotyczy w szczególności wdrażania usług certyfikacyjnych – na podstawie odpowiednich specyfikacji. Wymaga to przejrzystości i możliwości weryfikacji wdrożenia wymogów akredytacyjnych przez jednostkę certyfikującą oraz stałego utrzymywania zgodności z nimi.

W tym celu w systemie zarządzania należy określić metody wypełniania i kontrolowania tych wymogów zgodnie z przepisami o ochronie danych oraz metody ciągłej kontroli tych wymogów przez samą jednostkę akredytowaną.

Te zasady zarządzania i ich udokumentowane wdrażanie muszą być przejrzyste i ujawniane przez akredytowany podmiot certyfikujący w ramach procedury akredytacji zgodnie z art. 58, a następnie na wniosek organu nadzorczego ds. ochrony danych w każdym momencie podczas dochodzenia

w formie przeglądów w zakresie ochrony danych na podstawie art. 58 ust. 1 lit. b) lub przeglądu – na podstawie art. 58 ust. 1 lit. c) – certyfikacji udzielonych na mocy art. 42 ust. 7.

Akredytowana jednostka certyfikująca musi w szczególności stale podawać do wiadomości publicznej, które certyfikacje (lub mechanizmy bądź systemy certyfikacji) zostały przeprowadzone na jakiej podstawie oraz jaki jest okres ważności certyfikacji na podstawie jakich ram i warunków (motyw 100).

8.1 Ogólne wymogi dotyczące systemu zarządzania

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.2 Dokumentacja systemu zarządzania

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.3 Kontrola dokumentów

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.4 Kontrola ewidencji

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.5 Przegląd systemu zarządzania

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.6 Audyty wewnętrzne

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.7 Działania naprawcze

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.8 Działania zapobiegawcze

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

9 DALSZE DODATKOWE WYMOGI[21]

9.1 Aktualizacja metod oceny

Podmiot certyfikujący ustanawia procedury aktualizacji metod oceny stosowanych w kontekście oceny, o której mowa w pkt 7.4. Aktualizacja musi następować w kontekście zmian ram prawnych, odnośnego ryzyka, aktualnego stanu wiedzy oraz kosztów wdrożenia środków technicznych i organizacyjnych.

[21] Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

9.2 Utrzymywanie wiedzy fachowej

Jednostki certyfikujące ustanawiają procedury służące zapewnieniu szkolenia pracowników w celu aktualizacji ich umiejętności, z uwzględnieniem zmian, o których mowa w pkt 9.1.

9.3 Zakresy odpowiedzialności i kompetencji

9.3.1 Komunikacja między podmiotem certyfikującym a jego klientami

Zapewnia się istnienie procedur wdrażania odpowiednich procedur i struktur komunikacyjnych między podmiotem certyfikującym a klientem. Obejmują one:

1. prowadzenie przez akredytowany podmiot certyfikujący dokumentacji zadań i obowiązków do celów:
    a. odpowiadania na wnioski o udzielenie informacji lub
    b. umożliwienia kontaktu w przypadku skargi dotyczącej certyfikacji;
2. prowadzenie procesu przyjmowania wniosków w celu:
    a. udzielania informacji o postępie w rozpatrywaniu wniosku;
    b. przeprowadzania przez właściwy organ nadzorczy oceny dotyczącej:
        i. informacji zwrotnej;
        ii. decyzji właściwego organu nadzorczego.

9.3.2 Dokumentacja działalności w zakresie oceny

Organ nadzorczy może sformułować dodatkowe wymogi.

9.3.3 Zarządzanie rozpatrywaniem skarg

Rozpatrywanie skarg powinno stanowić integralną część systemu zarządzania, zgodną w szczególności z wymogami pkt 4.1.2.2 lit. c), 4.1.2.2 lit. j), 4.6 lit. d) i 7.13 normy ISO/IEC 17065/2012.

Odpowiednie skargi i sprzeciwy należy zgłaszać właściwemu organowi nadzorczemu.

9.3.4 Zarządzanie cofaniem akredytacji

Procedury w przypadku zawieszenia lub cofnięcia akredytacji włącza się do systemu zarządzania podmiotu certyfikującego, co obejmuje powiadamianie klientów.