Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia

Wersja 3.0

4 czerwca 2019 r.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Tekst przyjęty

Historia wersji

Wersja 3.0	4 czerwca 2019 r.	Włączenie załącznika 2 (wersja 2.0 załącznika 2 przyjęta w dniu 4 czerwca 2019 r. po konsultacjach publicznych)
Wersja 2.1	9 kwietnia 2019 r.	Przyjęcie sprostowania do wytycznych (pkt 45)
Wersja 2.0	23 stycznia 2019 r.	Przyjęcie wytycznych po przeprowadzeniu konsultacji publicznych – W tym samym dniu załącznik 2 (wersja 1.0) został przyjęty do konsultacji publicznych.
Wersja 1.0	25 maja 2018 r.	Przyjęcie wytycznych do konsultacji w sprawie publikacji

Spis treści

Europejska Rada Ochrony Danych,

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 (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego z dnia 25 maja 2018 r.,

biorąc pod uwagę wyniki konsultacji publicznych w sprawie wytycznych, które odbyły się w dniach 30 maja 2018 r. – 12 lipca 2018 r., oraz w sprawie załącznika 2, które odbyły się w dniach 15 lutego – 29 marca 2019 r., zgodnie z art. 70 ust. 4 RODO,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1 WPROWADZENIE

1. W ogólnym rozporządzeniu o ochronie danych (rozporządzenie 2016/279, „RODO" lub „rozporządzenie") przedstawiono zmodernizowane ramy zgodności z przepisami dotyczącymi rozliczalności i praw podstawowych do celów ochrony danych w Europie. Kluczowe znaczenie w tych nowych ramach ma szereg środków, które ułatwiają przestrzeganie przepisów RODO. Środki te obejmują obowiązkowe wymogi w określonych okolicznościach (w tym powołanie inspektorów ochrony danych i przeprowadzenie ocen skutków dla ochrony danych) oraz dobrowolne środki takie jak kodeksy postępowania i mechanizmy certyfikacji.
2. Przed przyjęciem RODO Grupa Robocza Art. 29 ustaliła, że certyfikacja może odgrywać istotną rolę w ramach rozliczalności do celów ochrony danych[1]. Aby za pomocą certyfikacji zapewnić wiarygodne dowody na zgodność z przepisami o ochronie danych, należy wprowadzić jasne zasady określające wymogi dotyczące świadczenia usług certyfikacyjnych[2]. W art. 42 RODO zapewniono podstawę prawną dotyczącą opracowania takich zasad.
3. Art. 42 ust. 1 RODO stanowi, że:

   „Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Przy tym uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw".

[1] Grupa Robocza Art. 29, opinia 3/2010 w sprawie zasady rozliczalności, WP173, 13 lipca 2010 r., pkt 69–71.
[2] Grupa Robocza Art. 29, opinia 3/2010 w sprawie zasady rozliczalności, WP173, pkt 69.

4. Mechanizmy certyfikacji3 mogą przyczynić się do poprawy przejrzystości dla osób, których dane dotyczą, a także do poprawy stosunków między przedsiębiorstwami, np. między administratorami i podmiotami przetwarzającymi. W motywie 100 RODO stwierdzono, że ustanowienie mechanizmów certyfikacji może zwiększyć przejrzystość i poprawić przestrzeganie rozporządzenia oraz pozwolić w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi4.

5. W RODO nie wprowadza się prawa ani obowiązku certyfikacji dla administratorów i podmiotów przetwarzających; zgodnie z art. 42 ust. 3 certyfikacja jest procesem dobrowolnym, który ma pomóc w wykazaniu przestrzegania RODO. Państwa członkowskie oraz organy nadzorcze wzywa się do zachęcania do ustanawiania mechanizmów certyfikacji; określą też one zaangażowanie zainteresowanych stron w proces certyfikacji oraz cykl życia certyfikacji.

6. Ponadto zgodność z zatwierdzonymi mechanizmami certyfikacji jest czynnikiem, który organy nadzorcze muszą brać pod uwagę jako czynnik obciążający lub łagodzący, gdy decydują się na zastosowanie administracyjnej kary pieniężnej oraz kiedy ustalają wysokość tej kary (art. 83 ust. 2 lit. j))5.

1.1 Zakres wytycznych

7. Niniejsze wytyczne mają ograniczony zakres; nie są one podręcznikiem procedur dotyczących certyfikacji zgodnie z RODO. Głównym celem niniejszych wytycznych jest określenie nadrzędnych wymogów i kryteriów, które mogą mieć zastosowanie do wszystkich rodzajów mechanizmów certyfikacji opracowanych zgodnie z art. 42 i 43 RODO. W tym celu w wytycznych:

   - zbadano zasadność certyfikacji jako narzędzia rozliczalności;
   - wyjaśniono kluczowe pojęcia zastosowane w przepisach dotyczących certyfikacji zawartych w art. 42 i 43; a także
   - wyjaśniono zakres możliwych przedmiotów certyfikacji zgodnie z art. 42 i 43 oraz cel certyfikacji;
   - ułatwiono uzyskiwanie miarodajnych, jednoznacznych, możliwie jak najbardziej powtarzalnych i porównywalnych wyników certyfikacji, niezależnie od jednostki certyfikującej (porównywalność).

8. W RODO zezwala się państwom członkowskim i organom nadzorczym na wdrażanie przepisów art. 42 i 43 na wiele sposobów. W wytycznych przedstawiono porady dotyczące interpretacji i wdrażania przepisów art. 42 i 43, co pomoże państwom członkowskim,

[3] Niniejsze wytyczne będą odnosiły się do mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych łącznie jako do „mechanizmów certyfikacji", zob. sekcja 1.3.2.
[4] W motywie 100 stwierdzono, że należy zachęcać do ustanowienia mechanizmów certyfikacji, aby zwiększyć przejrzystość i poprawić przestrzeganie rozporządzenia, pozwalając w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi.
[5] Zob. Grupa Robocza Art. 29, Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia 2016/679, (WP 253).

organom nadzorczym oraz krajowym jednostkom akredytującym w ustanowieniu bardziej spójnego, zharmonizowanego podejścia do wdrażania mechanizmów certyfikacji zgodnie z RODO.

9. Porady zawarte w wytycznych będą istotne dla:

   - właściwych organów nadzorczych oraz dla Europejskiej Rady Ochrony Danych („EROD") przy zatwierdzaniu kryteriów certyfikacji na podstawie art. 42 ust. 5, art. 58 ust. 3 lit. f) oraz art. 70 ust. 1 lit. o);
   - podmiotów certyfikujących przy określaniu i dokonywaniu przeglądu kryteriów certyfikacji przed przedłożeniem ich do zatwierdzenia właściwemu organowi nadzorczemu zgodnie z art. 42 ust. 5;
   - EROD przy zatwierdzaniu europejskiego znaku jakości ochrony danych na podstawie art. 42 ust. 5 i art. 70 ust. 1 lit. o);
   - organów nadzorczych przy opracowywaniu ich własnych kryteriów certyfikacji;
   - Komisji Europejskiej, która jest uprawniona do przyjmowania aktów delegowanych w celu doprecyzowania wymogów uwzględnianych w odniesieniu do mechanizmów certyfikacji na podstawie art. 43 ust. 8;
   - EROD podczas udzielania Komisji Europejskiej opinii w sprawie wymogów certyfikacyjnych zgodnie z art. 70 ust. 1 lit. q) i art. 43 ust. 8;
   - krajowych jednostek akredytujących, które będą musiały brać pod uwagę kryteria certyfikacji z myślą o akredytacji podmiotów certyfikujących zgodnie z normą EN-ISO/IEC 17065/2012, a także dodatkowe wymogi zgodnie z art. 43; a także
   - administratorów i podmiotów przetwarzających przy określaniu ich własnej strategii zapewniania zgodności z RODO oraz rozważaniu certyfikacji jako sposobu wykazywania zgodności z przepisami.

10. EROD opublikuje osobne wytyczne dotyczące kwestii określania kryteriów zatwierdzania mechanizmów certyfikacji jako narzędzi przekazywania do państw trzecich lub organizacji międzynarodowych zgodnie z art. 42 ust. 2.

1.2 Cel certyfikacji na podstawie RODO

11. W art. 42 ust. 1 stwierdzono, że mechanizmy certyfikacji ustanawia się, by świadczyły „o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające".

12. RODO stanowi przykład kontekstu, w którym zatwierdzone mechanizmy certyfikacji można wykorzystywać do wykazania wypełnienia zobowiązań przez administratorów i podmioty przetwarzające, które to zobowiązania dotyczą:

   - wdrażania i wykazywania istnienia odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 24 ust. 1 i 3, art. 25 oraz art. 32 ust. 1 i 3;

- wystarczających gwarancji (ze strony podmiotu przetwarzającego względem administratora), o których mowa w art. 28 ust. 5 akapit 1 oraz (ze strony jednego podmiotu przetwarzającego względem innego podmiotu przetwarzającego) w art. 28 ust. 5 akapit 4.

13. Ponieważ za pomocą certyfikacji samej w sobie nie można udowodnić zgodności z przepisami, a stanowi ona raczej element, który można wykorzystać w celu wykazania zgodności, należy jej dokonywać w sposób przejrzysty. Wykazanie zgodności wymaga posiadania dokumentów potwierdzających, specjalnie w tym celu sporządzonych sprawozdań, w których nie tylko zostaną powtórzone kryteria, ale będzie też opisane, w jaki sposób są one spełniane, oraz – jeżeli nie były spełniane od początku – jakie korekty i działania naprawcze wprowadzono, jak również stosowność takich korekt i działań; tym samym zostaną przedstawione powody przyznania i utrzymania certyfikacji. Powyższe obejmuje zarys indywidualnej decyzji dotyczącej udzielenia, przedłużenia lub cofnięcia certyfikatu. W dokumentach tych powinny znaleźć się powody, argumenty i dowody wynikające z zastosowania kryteriów oraz konkluzje, sądy lub wnioski sformułowane na podstawie faktów lub przesłanek zgromadzonych podczas certyfikacji.

1.3 Kluczowe pojęcia

14. W niniejszej sekcji przeanalizowano kluczowe pojęcia zawarte w art. 42 i 43. W analizie tej rozwinięto rozumienie podstawowych terminów oraz zakresu certyfikacji na podstawie RODO.

1.3.1 Interpretacja „certyfikacji”

15. W RODO nie zdefiniowano terminu „certyfikacja”. Międzynarodowa Organizacja Normalizacyjna (ISO) przedstawia uniwersalną definicję pojęcia certyfikacji jako „dostarczenia przez niezależny organ pisemnego zapewnienia (certyfikatu), że dany produkt, usługa lub system spełnia określone wymagania”. Certyfikacja jest również nazywana „oceną zgodności przez stronę trzecią”, a podmioty certyfikujące mogą być również nazywane „jednostkami oceniającymi zgodność”. W normie EN-ISO/IEC 17000:2004 – Ocena zgodności – Słownictwo i ogólne zasady (do których odwołuje się norma ISO17065) – certyfikację definiuje się w następujący sposób: „Zaświadczenie przez osobę trzecią (...) związane z produktami, procesami i usługami”.

16. Zaświadczenie jest „kwestią oświadczenia na podstawie podjętej po przeglądzie decyzji, że wykazano spełnienie określonych wymagań” (rozdział 5.2, ISO 17000: 2004).

17. W kontekście certyfikacji na podstawie art. 42 i 43 RODO certyfikacja dotyczy zaświadczenia osoby trzeciej odnoszącego się do operacji przetwarzania dokonywanych przez administratorów i podmioty przetwarzające.

1.3.2 Mechanizmy certyfikacji, znaki jakości i oznaczenia

18. W RODO nie zdefiniowano „mechanizmów certyfikacji, znaków jakości i oznaczeń", a terminy te stosuje się łącznie. Certyfikat jest oświadczeniem o zgodności. Znak jakości lub oznaczenie można wykorzystać w celu potwierdzenia pomyślnego zakończenia procedury certyfikacji. Znak jakości lub oznaczenie najczęściej odnosi się do logo lub symbolu, których obecność (poza certyfikatem) świadczy o tym, że przedmiot certyfikacji poddano niezależnej ocenie oraz że spełnia on dane wymogi określone w dokumentach normatywnych, takich jak przepisy, normy lub specyfikacje techniczne. Wymogi te w kontekście certyfikacji na podstawie RODO określono w dodatkowych wymaganiach, które stanowią uzupełnienie zasad akredytacji podmiotów certyfikujących zawartych w normie EN-ISO/IEC 17065/2012 oraz kryteriów certyfikacji zatwierdzonych przez właściwy organ nadzorczy lub EROD. Certyfikat, znak jakości lub oznaczenie na podstawie RODO mogą zostać przyznane wyłącznie po przeprowadzeniu przez akredytowany podmiot certyfikujący lub właściwy organ nadzorczy niezależnej oceny dowodów, w której zostanie stwierdzone, że spełniono kryteria certyfikacji.

19. W tabeli przedstawiono ogólny przykład procesu certyfikacji.

Złożenie wniosku przez administratora lub podmiot przetwarzający	**Formalne sprawdzenie przez podmiot certyfikujący**	**Ocena** **Wstępna ocena**	**Ocena** **Ewaluacja przedmiotu oceny**	**Ocena** **Zatwierdzenie wyników**	**Informacja dla właściwego organu nadzorczego**	**Certyfikacja**	**Monitorowanie**	**Przedłużenie certyfikacji**
Czy opis przedmiotu oceny jest jednoznaczny i kompletny, w tym w odniesieniu do interfejsów?	Czy opis przedmiotu oceny może zostać zaakceptowany?	Jakie kryteria są stosowane?	Czy przedmiot oceny spełnia kryteria?	Czy wszystkie istotne kryteria określono tak, by odzwierciedlić przedmiot oceny?	Czy przedstawiono powody udzielenia lub cofnięcia certyfikacji?	Czy można przyznać certyfikat?	Czy przedmiot oceny w dalszym ciągu spełnia kryteria?	Czy przetwarzanie danych wciąż spełnia kryteria certyfikacji?
Czy można zapewnić dostęp do czynności przetwarzania dotyczących przedmiotu oceny?	Czy wszystkie dokumenty są kompletne i aktualne?	Jakie metody oceny są stosowane?	Czy dokumentacja dotycząca przedmiotu oceny jest prawidłowa?	Czy ocenę udokumentowano w wystarczający sposób?		Czy sprawozdania są gotowe do publikacji?	Czy certyfikat / znak jakości / znak zaufania jest poprawnie używany?	Czy podjęto zadowalające działania w odniesieniu do obszarów wymagających rozwoju?
Art. 42 ust. 6	Art. 43 ust. 4	Art. 43 ust. 4	Art. 42 ust. 5, art. 43 ust. 4	Art. 43 ust. 4	Art. 43 ust. 1, art. 43 ust. 5	Art. 43 ust. 1, art. 42 ust. 7	Art. 42 ust. 7	Art. 42 ust. 7

2 ROLA ORGANÓW NADZORCZYCH

20. Art. 42 ust. 5 stanowi, że certyfikacji dokonuje akredytowany podmiot certyfikujący lub właściwy organ nadzorczy. Zgodnie z RODO udzielanie certyfikacji nie jest obowiązkowym zadaniem organów nadzorczych. W RODO dopuszcza się natomiast wiele różnych modeli. Organ nadzorczy może na przykład wybrać co najmniej jedną z następujących możliwości:

    - może sam udzielać certyfikacji na podstawie własnego systemu certyfikacji;
    - może sam udzielać certyfikacji na podstawie własnego systemu certyfikacji, ale przekazać cały proces oceny lub część tego procesu osobom trzecim;

- może opracować własny system certyfikacji i powierzyć procedurę certyfikacji podmiotom certyfikującym, które będą certyfikacji udzielać; a także
- może zachęcać rynek do tworzenia mechanizmów certyfikacji.

21. Organ nadzorczy będzie również musiał rozpatrzyć swoją rolę w świetle decyzji dotyczących mechanizmów akredytacji podjętych na szczeblu krajowym – zwłaszcza jeżeli sam organ nadzorczy jest uprawniony do akredytowania podmiotów certyfikujących na podstawie art. 43 ust. 1 RODO. Tym samym każdy organ nadzorczy określi, jakie podejście przyjąć w celu realizacji szerokiego zamiaru certyfikacji na podstawie RODO. Zostanie to określone nie tylko w kontekście zadań i uprawnień wymienionych w art. 57 i 58, ale również przy uwzględnianiu certyfikacji jako czynnika, który należy brać pod uwagę przy ustalaniu administracyjnych kar pieniężnych oraz bardziej ogólnie jako sposobu wykazywania zgodności.

2.1 Organ nadzorczy jako podmiot certyfikujący

22. Jeżeli organ nadzorczy zdecyduje się na prowadzenie certyfikacji, będzie musiał starannie ocenić swoją rolę w stosunku do przypisanych mu zadań na podstawie RODO. Jego rola w wykonywaniu swoich funkcji powinna być przejrzysta. Będzie on musiał rozważyć w szczególności rozdzielenie uprawnień dotyczących postępowań i egzekwowania przepisów w celu uniknięcia wszelkich potencjalnych konfliktów interesów.

23. Działając jako podmiot certyfikujący, organ nadzorczy będzie musiał zapewnić utworzenie właściwego mechanizmu certyfikacji i opracować własne kryteria certyfikacji lub takie kryteria przyjąć. Ponadto każdy organ nadzorczy udzielający certyfikacji ma za zadanie okresowo dokonywać ich przeglądu (art. 57 ust. 1 lit. o)) oraz jest uprawniony do cofnięcia certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane (art. 58 ust. 2 lit. h)). Aby spełnić te wymogi, przydatne jest opracowanie procedury certyfikacji oraz wymogów procesu certyfikacji, a także, jeżeli nie ustalono inaczej np. w prawie krajowym, wprowadzić prawnie wiążącą umowę o świadczenie usług certyfikacyjnych z indywidualną organizacją wnioskodawcy. Należy zapewnić, by w takiej umowie dotyczącej certyfikacji wymagano od wnioskodawcy spełnienia co najmniej kryteriów certyfikacji, w tym koniecznych ustaleń dotyczących prowadzenia oceny, monitorowania spełnienia kryteriów oraz dokonywania przeglądu okresowego, w tym dostępu do informacji lub pomieszczeń, dokumentacji i publikacji sprawozdań i wyników oraz rozpatrywania skarg. Ponadto oczekuje się, że poza wymogami wymienionymi w art. 43 ust. 2 organ nadzorczy spełni wymogi określone w wytycznych w sprawie akredytacji podmiotów certyfikujących.

2.2 Dalsze zadania organu nadzorczego w odniesieniu do certyfikacji

24. W państwach członkowskich, w których podmioty certyfikujące podejmują działalność, organ nadzorczy posiada niezależnie od własnej działalności zadania i uprawnienia, takie jak:
    - ocena kryteriów systemu certyfikacji oraz przygotowanie projektu decyzji (art. 42 ust. 5);

- przekazanie EROD projektu decyzji, kiedy Rada będzie poweźmie zamiar o zatwierdzeniu kryteriów certyfikacji (art. 64 ust. 1 lit. c), art. 64 ust. 7) oraz uwzględnienie opinii Rady (art. 64 ust. 1 lit. c), art. 70 ust. 1 lit. t));
- zatwierdzenie kryteriów certyfikacji (art. 58 ust. 3 lit. f)) zanim nastąpi akredytacja i certyfikacja (art. 42 ust. 5 i art. 43 ust. 2 lit. b));
- publikacja kryteriów certyfikacji (art. 43 ust. 6);
- działanie jako właściwy organ w odniesieniu do ogólnounijnych systemów certyfikacji, co może skutkować europejskim znakiem jakości ochrony danych zatwierdzonym przez EROD (art. 42 ust. 5 i art. 70 ust. 1 lit. o)); oraz a także
- nakazanie podmiotowi certyfikującemu a) nieudzielania certyfikacji lub b) cofnięcia certyfikacji, jeżeli jej wymogi (procedury dotyczące certyfikacji lub jej kryteria) nie są spełnione lub przestały być spełniane (art. 58 ust. 2 lit. h)).

25. W RODO powierza się organom nadzorczym zadanie polegające na zatwierdzaniu kryteriów certyfikacji, ale nie na opracowywaniu tych kryteriów. Aby zatwierdzić kryteria certyfikacji na podstawie art. 42 ust. 5, organ nadzorczy powinien dokładnie rozumieć, czego ma oczekiwać, zwłaszcza jeżeli chodzi o zakres oraz treść potrzebne do wykazania zgodności z RODO, oraz w odniesieniu do swojego zadania, jakim jest monitorowanie i egzekwowanie stosowania rozporządzenia. W załączniku zawarto wskazówki mające na celu zapewnienie zharmonizowanego podejścia podczas dokonywania oceny kryteriów w celu zatwierdzenia.

26. W art. 43 ust. 1 wymaga się, by podmioty certyfikujące informowały swój organ nadzorczy przed udzieleniem lub przedłużeniem certyfikacji, by umożliwić właściwemu organowi nadzorczemu wykonywanie jego uprawnień naprawczych na mocy art. 58 ust. 2 lit. h). Ponadto w art. 43 ust. 5 wymaga się również, by podmioty certyfikujące przedstawiały właściwemu organowi nadzorczemu powody udzielenia lub cofnięcia żądanej certyfikacji. Mimo że w RODO pozwala się organom nadzorczym określić, w jaki sposób będą otrzymywać informacje, uznawać je, dokonywać ich przeglądu oraz operacyjnego przetwarzania (np. może to obejmować rozwiązania technologiczne mające na celu umożliwienie realizowania sprawozdawczości przez podmioty certyfikujące), istnieje możliwość wprowadzenia procesu i kryteriów przetwarzania informacji i sprawozdań przekazanych na temat każdego udanego projektu certyfikacji przez podmiot certyfikujący zgodnie z art. 43 ust. 1. Na podstawie tych informacji organ nadzorczy może wykonać swoje uprawnienie do nakazania podmiotowi certyfikującemu cofnięcia lub nieudzielenia certyfikacji (art. 58 ust. 2 lit. h)) oraz do monitorowania i egzekwowania stosowania wymogów i kryteriów certyfikacji na podstawie RODO (art. 57 ust. 1 lit. a) i art. 58 ust. 2 lit. h)). Będzie to służyć wspieraniu zharmonizowanego podejścia oraz porównywalności w certyfikacji przez poszczególne podmioty certyfikujące oraz zapewnieniu, by informacje o statusie certyfikacji organizacji były znane organom nadzorczym.

3 ROLA PODMIOTU CERTYFIKUJĄCEGO

27. Rolą podmiotu certyfikującego jest udzielanie certyfikacji, dokonywanie ich przeglądu, przedłużanie ich i cofanie (art. 42 ust. 5 i 7) na podstawie mechanizmu certyfikacji i zatwierdzonych kryteriów (art. 43 ust. 1). Wymaga to od podmiotu certyfikującego lub właściciela systemu certyfikacji określenia i ustanowienia kryteriów i procedur certyfikacji, w tym procedur dotyczących monitorowania przestrzegania rozporządzenia, przeglądu, rozpatrywania skarg oraz cofania certyfikacji. Przeglądu kryteriów certyfikacji dokonuje się w ramach procesu akredytacji uwzględniającego zasady i procedury, na podstawie których wydaje się certyfikacje, znaki jakości i oznaczenia (art. 43 ust. 2 lit. c)).

28. Istnienie mechanizmów i kryteriów certyfikacji jest konieczne, by podmiot certyfikujący mógł otrzymać akredytację na podstawie art. 43. Istotny wpływ na to, co robi podmiot certyfikujący, wynika z zakresu i rodzaju kryteriów certyfikacji, które mają wpływ na procedury certyfikacji i vice versa. Specyficzne kryteria mogą na przykład wymagać konkretnych metod oceny, takich jak kontrole na miejscu i przegląd kodu. Procedury te są w przypadku akredytacji obowiązkowe; wyjaśniono je bardziej szczegółowo w wytycznych w sprawie akredytacji.

29. W RODO wymaga się, by podmiot certyfikujący przekazywał organom nadzorczym informacje, w szczególności na temat poszczególnych certyfikacji, które to informacje są konieczne do monitorowania stosowania mechanizmu certyfikacji (art. 42 ust. 7, art. 43 ust. 5 i art. 58 ust. 2 lit. h)).

4 ZATWIERDZENIE KRYTERIÓW CERTYFIKACJI

30. Kryteria certyfikacji stanowią integralną część każdego mechanizmu certyfikacji. W konsekwencji w RODO wymaga się zatwierdzenia kryteriów certyfikacji mechanizmu certyfikacji przez właściwy organ nadzorczy (art. 42 ust. 5 i art. 43 ust. 2 lit. b)). Natomiast w przypadku europejskiego znaku jakości ochrony danych kryteria certyfikacji zatwierdza EROD (art. 42 ust. 5 i art. 70 ust. 1 lit. o)). Obie procedury zatwierdzania kryteriów certyfikacji wyjaśniono poniżej.

31. EROD uznaje następujące cele zatwierdzania kryteriów certyfikacji:

- odpowiednie odzwierciedlenie wymów i zasad dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, które to wymogi i zasady określono w rozporządzeniu (UE) 2016/679; a także
- przyczynianie się do spójnego stosowania RODO.

32. Zatwierdzenia udziela się na podstawie wymogu RODO, by mechanizm certyfikacji umożliwiał administratorom i podmiotom przetwarzającym wykazanie zgodności z RODO; kryteria certyfikacji mają w pełni ten wymóg odzwierciedlać.

4.1 Zatwierdzenie kryteriów przez właściwy organ nadzorczy

33. Właściwy organ nadzorczy musi zatwierdzać kryteria certyfikacji przed rozpoczęciem procesu akredytacji podmiotu certyfikującego lub w trakcie tego procesu. Wymagane jest również zatwierdzenie zaktualizowanych lub dodatkowych systemów lub zbiorów kryteriów na

podstawie normy ISO 17065 przez ten sam podmiot certyfikujący przed zastosowaniem ich w ramach zmienionych mechanizmów certyfikacji (art. 42 ust. 5 i art. 43 ust. 2 lit. b)). Organy nadzorcze traktują wszystkie wnioski o zatwierdzenie kryteriów certyfikacji w sposób sprawiedliwy i niedyskryminujący zgodnie z publicznie dostępną procedurą określającą ogólne warunki, które należy spełnić, oraz zgodnie z opisem procesu zatwierdzania.

34. Podmiot certyfikujący może udzielać certyfikacji w danym państwie członkowskim jedynie zgodnie z kryteriami przyjętymi przez organ nadzorczy w tym państwie członkowskim. Innymi słowy, jeżeli podmiot certyfikujący zamierza oferować certyfikację i uzyska akredytację, kryteria certyfikacji musi zatwierdzać właściwy organ nadzorczy. W sekcji poniżej podano więcej informacji na temat ogólnoeuropejskich systemów certyfikacji.

4.2 Zatwierdzanie przez EROD kryteriów dotyczących europejskiego znaku jakości ochrony danych

35. Podmiot certyfikujący może również udzielać certyfikacji zgodnie z kryteriami zatwierdzonymi przez EROD w odniesieniu do europejskiego znaku jakości ochrony danych. Zatwierdzenie kryteriów certyfikacji przez EROD zgodnie z art. 63 może skutkować europejskim znakiem jakości ochrony danych (art. 42 ust. 5). W świetle istniejącej certyfikacji i konwencji w sprawie akredytacji EROD uznaje, że pożądane jest unikanie fragmentacji rynku certyfikacji ochrony danych osobowych. Rada zauważa, że art. 42 ust. 1 stanowi, iż państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do ustanawiania mechanizmów certyfikacji – w szczególności na szczeblu Unii.

4.2.1 Wniosek o zatwierdzenie

36. Wniosek o zatwierdzenie przez EROD kryteriów zgodnie z art. 42 ust. 5 i art. 70 ust. 1 lit. o) musi być złożony za pośrednictwem właściwego organu nadzorczego; w takim wniosku należy określić zamiar właściciela systemu, kandydata lub akredytowanego podmiotu certyfikującego, polegający na zaoferowaniu w mechanizmie certyfikacji kryteriów, które odnosiłyby się do administratorów i podmiotów przetwarzających we wszystkich państwach członkowskich. Właściwy organ nadzorczy przekaże EROD projekt, kiedy uzna, że EROD mogłaby zatwierdzić kryteria.

37. Wybór miejsca, w którym należy złożyć wniosek o zatwierdzenie kryteriów, będzie zależał od właścicieli systemu certyfikacji lub siedziby podmiotu certyfikującego.

38. Jeżeli podmiot certyfikujący złoży wniosek, zazwyczaj będzie już trwał w odniesieniu do niego proces ubiegania się o akredytację lub podmiot ten będzie już akredytowany przez właściwy organ nadzorczy albo przez krajową jednostkę akredytującą swojego państwa członkowskiego. Jeżeli podmiot certyfikujący został już akredytowany na potrzeby mechanizmu certyfikacji RODO, może to pomóc w usprawnieniu procesu zatwierdzania.

4.2.2 Kryteria dotyczące europejskiego znaku jakości ochrony danych

39. EROD będzie koordynować proces oceny oraz zatwierdzenia europejskiego znaku jakości ochrony danych zgodnie z wymogami. Ocena będzie dotyczyła takich obszarów, jak: zakres kryteriów oraz możliwość ich wykorzystania do wspólnej certyfikacji. Oczekuje się, że jeżeli EROD zatwierdzi kryteria, organ nadzorczy właściwy dla siedziby unijnej podmiotu certyfikującego będzie rozpatrywać skargi odnoszące się do samego mechanizmu oraz poinformuje pozostałe organy nadzorcze. Ten organ nadzorczy jest również właściwy do podejmowania środków przeciwko podmiotowi certyfikującemu. W zależności od sytuacji właściwy organ nadzorczy powiadomi pozostałe organy nadzorcze oraz EROD.

40. Kryteria certyfikacji dotyczące wspólnej certyfikacji podlegają ogólnounijnym wymogom i powinny zapewniać specjalny mechanizm służący do spełnienia tych wymogów. Europejskie mechanizmy certyfikacji muszą być przeznaczone do stosowania we wszystkich państwach członkowskich. Na podstawie art. 42 ust. 5 powinno być możliwe dostosowanie mechanizmu dotyczącego europejskiego znaku jakości ochrony danych oraz jego kryteriów w taki sposób, by w stosownych przypadkach uwzględniano w nich krajowe przepisy sektorowe, np. dotyczące przetwarzania danych w szkołach; należy również brać pod uwagę zastosowanie ich w całej Europie.

41. Na przykład: międzynarodowa szkoła oferująca w Unii szkolenie osób, których dane dotyczą, znajduje się w państwie członkowskim „A”. Szkoła chce poświadczyć swój proces internetowego składania wniosków za pomocą ogólnounijnego systemu certyfikacji, aby uzyskać europejski znak jakości ochrony danych. Szkoła ta ma zamiar ubiegać się o certyfikację operacji przetwarzania oferowaną przez podmiot certyfikujący ustanowiony w państwie członkowskim „B” na podstawie europejskiego znaku jakości ochrony danych. Kryteria dotyczącego tego znaku, które opracowano i udokumentowano w odpowiednim mechanizmie, muszą być w stanie uwzględnić przepisy dotyczące szkół mające zastosowanie w państwie członkowskim „A”. W ramach tych kryteriów należy również wymagać stosowania przez szkołę internetowego procesu składania wniosków w celu przekazania informacji i uwzględnienia mających zastosowanie wymogów państwa członkowskiego dotyczących ochrony danych, które to wymogi mogą się różnić w zależności od państwa członkowskiego. Przykładem są zbiory danych osobowych, które mają zostać przekazane do celów wniosku, np. klasy przedszkolne lub wyniki testów, różne okresy zatrzymywania danych, gromadzenie lub przetwarzanie danych finansowych lub biometrycznych, dalsze ograniczenia w zakresie przetwarzania.

- Ogólne kryteria dotyczące zatwierdzania mechanizmu europejskiego znaku jakości ochrony danych obejmują:
  - kryteria zatwierdzone przez Europejską Radę Ochrony Danych;
  - zastosowanie ich we wszystkich jurysdykcjach w sposób odzwierciedlający, w stosownych przypadkach, krajowe wymogi prawne i przepisy sektorowe;
  -
- zharmonizowane kryteria, które można dostosowywać w celu odzwierciedlenia wymogów krajowych;
  - opis mechanizmu certyfikacji określający;

- umowy w sprawie certyfikacji, w których uwzględnia się wymogi ogólnoeuropejskie;
- procedury mające na celu zapewnienie i dostarczenie rozwiązań dla różnych krajowych uwarunkowań oraz zapewnienie, by europejski znak jakości pomagał w wykazywaniu zgodności z RODO; a także
- język sprawozdań składanych do wszystkich odnośnych organów nadzorczych.

42. Porady dotyczące kryteriów europejskiego znaku jakości ochrony danych zawiera również załącznik.

4.2.3 Rola akredytacji

43. Jak zauważono w puncie 4.2.1, kiedy kryteria zostaną zidentyfikowane jako stosowne w odniesieniu do wspólnej certyfikacji, a Europejska Rada Ochrony Danych zatwierdzi je jako takie zgodnie z art. 42 ust. 5, podmioty certyfikujące mogą być akredytowane do prowadzenia certyfikacji na podstawie tych kryteriów na poziomie Unii.

44. Systemy, które są przeznaczone do stosowania jedynie w konkretnych państwach członkowskich, nie będą kandydatami do przyznania unijnych znaków jakości. Akredytacja w zakresie europejskiego znaku jakości ochrony danych będzie wymagała akredytacji w państwie członkowskim siedziby podmiotu certyfikującego, który ma zamiar obsługiwać system, tj. podmiotu odpowiedzialnego za udzielanie certyfikacji i zarządzanie działalnością certyfikacyjną swoich podmiotów i jednostek zależnych w innych państwach członkowskich. Jeżeli inne jednostki organizacyjne lub biura zarządzają certyfikacjami i wykonują je samodzielnie, każda z tych jednostek organizacyjnych lub biur będzie wymagać osobnej akredytacji w państwie członkowskim, w którym ma swoją siedzibę. Innymi słowy, akredytacja jest konieczna jedynie w państwie członkowskim, w którym znajduje się siedziba podmiotu certyfikującego, tylko kiedy siedziba ta wydaje certyfikaty. Natomiast, gdy inne jednostki organizacyjne podmiotu certyfikującego również wydają certyfikaty, jednostki te także muszą posiadać akredytację.

45. W związku z tym, jeżeli podmiot certyfikujący nie został akredytowany do certyfikacji w ramach europejskiego znaku jakości ochrony danych, nie mogą mieć zastosowania kryteria zatwierdzone przez EROD i nie można zaoferować znaku jakości.

5 OPRACOWYWANIE KRYTERIÓW CERTYFIKACJI

46. W RODO ustanowiono ramy opracowywania kryteriów certyfikacji. Podczas gdy do podstawowych wymogów dotyczących procedury certyfikacji odnoszą się art. 42 i 43, w których przedstawiono również kluczowe kryteria dotyczące procedur certyfikacji,

podstawa kryteriów certyfikacji musi wynikać z zasad i przepisów RODO i pomóc w zapewnieniu stosowania tych zasad i przepisów.

47. Opracowywanie kryteriów certyfikacji powinno koncentrować się na możliwości zweryfikowania, istotności i stosowności kryteriów certyfikacji do celów wykazania zgodności z rozporządzeniem. Kryteria certyfikacji powinny być sformułowane w sposób jasny i zrozumiały oraz powinny umożliwiać ich praktyczne zastosowanie.

48. Podczas opracowywania kryteriów certyfikacji należy w stosownych przypadkach brać pod uwagę następujące aspekty zgodności wspierające ocenę operacji przetwarzania danych:

- zgodność przetwarzania z prawem, o której mowa w art. 6;
- zasady dotyczące przetwarzania danych, o których mowa w art. 5;
- prawa osób, których dane dotyczą, o których mowa w art. 12–23;
- obowiązek zgłaszania naruszeń ochrony danych zgodnie z art. 33;
- obowiązek uwzględniania ochrony danych w fazie projektowania oraz domyślną ochronę danych, zgodnie z art. 25;
- czy w stosownych przypadkach przeprowadzono ocenę skutków dla ochrony danych zgodnie z art. 35 ust. 7 lit. d); a także
- środki techniczne i organizacyjne wprowadzone zgodnie z art. 32.

49. Zakres, w jakim względy te odzwierciedlono w kryteriach, może być różny w zależności od zakresu certyfikacji, który może obejmować rodzaj operacji przetwarzania oraz obszar certyfikacji (np. sektor zdrowia).

5.1 Co może być przedmiotem certyfikacji na podstawie RODO?

50. EROD jest zdania, że w RODO przewidziano szeroki zakres możliwych przedmiotów certyfikacji na podstawie RODO, jeżeli nacisk kładzie się na pomoc w wykazaniu zgodności z rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające (art. 42 ust. 1).

51. Podczas oceny operacji przetwarzania należy w stosownych przypadkach uwzględnić następujące trzy kluczowe elementy:

1. dane osobowe (zakres przedmiotowy RODO);
2. systemy techniczne – infrastrukturę, np. sprzęt i oprogramowanie wykorzystywane do przetwarzania danych osobowych; a także
3. procesy i procedury związane z operacjami przetwarzania.

52. Każdy element wykorzystywany w operacjach przetwarzania musi podlegać ocenie w zestawieniu z ustalonymi kryteriami. Wpływ mogą mieć w tym przypadku co najmniej cztery różne istotne czynniki: 1) organizacja i struktura prawna administratora lub podmiotu

przetwarzającego; 2) dział, środowisko i osoby zaangażowane w operacje przetwarzania; 3) opis techniczny elementów podlegających ocenie; i wreszcie 4) infrastruktura informatyczna obsługująca operacje przetwarzania obejmująca systemy operacyjne, systemy wirtualne, bazy danych, systemy uwierzytelniania i autoryzacji, routery i zapory sieciowe, systemy magazynowania, infrastrukturę komunikacyjną lub dostęp do internetu oraz powiązane środki techniczne.

53. Wszystkie trzy podstawowe elementy są istotne przy opracowywaniu procedur i kryteriów certyfikacji. Zakres, w jakim się je uwzględnia, może różnić się w zależności od przedmiotu certyfikacji. Przykładowo w niektórych przypadkach pewne elementy można pominąć, jeżeli uzna się je za nieistotne dla przedmiotu certyfikacji.

54. W RODO zawarto dodatkowe wytyczne, na podstawie których można doprecyzować, co podlega certyfikacji na jego podstawie. Z art. 42 ust. 7 wynika, że certyfikacji na podstawie RODO udziela się wyłącznie administratorom danych i podmiotom przetwarzającym, co wyklucza między innymi możliwość udzielania certyfikacji inspektorom ochrony danych. W art. 43 ust. 1 lit. b) znajduje się odniesienie do normy ISO 17065, która przewiduję akredytację podmiotów certyfikujących dokonujących oceny wyrobów, usług i procesów. Operacja przetwarzania lub zestaw operacji mogą doprowadzić do powstania wyrobu lub usługi zgodnych z terminologią normy ISO 17065, a więc mogą być przedmiotem certyfikacji. Przykładowo przetwarzanie danych pracowników do celów wypłaty wynagrodzeń lub zarządzania urlopami w rozumieniu RODO stanowi zestaw operacji i może doprowadzić do powstania wyrobu, procesu lub usługi zgodnych z terminologią normy ISO.

55. Na podstawie powyższych ustaleń EROD uważa, że zakres certyfikacji na podstawie RODO jest ukierunkowany na operacje przetwarzania lub zestawy operacji. Powyższe może obejmować procesy zarządzania w rozumieniu środków organizacyjnych, a zatem procesy stanowiące integralne części operacji przetwarzania (np. proces zarządzania określony w odniesieniu do rozpatrywania skarg w ramach przetwarzania danych pracowników do celów wypłaty wynagrodzeń).

56. Aby ocenić zgodność operacji przetwarzania z kryteriami certyfikacji należy przedstawić przypadek użycia. Przykładowo zgodność stosowania infrastruktury technicznej wykorzystywanej w trakcie operacji przetwarzania zależy od kategorii danych, które infrastruktura ta ma przetwarzać. Stosowane środki organizacyjne zależą od kategorii i ilości danych oraz od infrastruktury technicznej wykorzystywanej do przetwarzania, z uwzględnieniem charakteru, zakresu, treści i celów przetwarzania, a także zagrożeń związanych z prawami i wolnościami osób, których dane dotyczą.

57. Ponadto należy pamiętać, że aplikacje informatyczne mogą się między sobą znacznie różnić, nawet jeśli służą tym samym celom związanym z przetwarzaniem danych. Dlatego należy to uwzględnić przy określaniu zakresu mechanizmów certyfikacji i sporządzaniu kryteriów certyfikacji, tj. zakresu certyfikacji i kryteriów nie należy zawężać tak, by spowodować wykluczenie zaprojektowanych w różny sposób aplikacji informatycznych.

5.2 Określenie przedmiotu certyfikacji

58. W przypadku poszczególnych projektów certyfikacyjnych prowadzonych w ramach mechanizmu certyfikacji należy odróżnić zakres mechanizmu certyfikacji od jej przedmiotu (zwanego również przedmiotem oceny). Mechanizm certyfikacji może określać jej zakres w sposób ogólny lub w odniesieniu do konkretnego rodzaju lub obszaru operacji przetwarzania, a zatem może już określać przedmioty certyfikacji, które mieszczą się w tym zakresie (np. bezpieczne magazynowanie i ochrona danych osobowych znajdujących się w cyfrowym sejfie). W każdym przypadku wiarygodna i sensowna ocena zgodności może mieć miejsce tylko wtedy, gdy dokładnie opisano indywidualny przedmiot projektu certyfikacyjnego. Należy jasno opisać, jakie operacje przetwarzania obejmuje przedmiot certyfikacji, po czym należy przedstawić opis podstawowych elementów, tj. które dane, procesy i infrastruktura techniczna będą poddawane ocenie, a które nie. Czyniąc to, należy zawsze również uwzględniać i opisywać powiązania z innymi procesami. Oczywiste jest, że to, czego nie wiadomo, nie może stanowić elementu oceny i w związku z tym nie może uzyskać certyfikatu. W każdym wypadku dany przedmiot certyfikacji musi być znaczący w stosunku do komunikatu lub roszczenia związanego z certyfikacją / wyrażonego za jej pośrednictwem i nie powinien wprowadzać użytkownika, klienta ani konsumenta w błąd.

59. [Przykład 1]

Bank oferuje swoim klientom stronę internetową, dzięki której mają oni dostęp do bankowości internetowej. W ramach tej usługi istnieje możliwość wykonywania przelewów, zakupu akcji, inicjowania zleceń stałych i zarządzania rachunkiem. Bank pragnie certyfikować następujące elementy w ramach mechanizmu certyfikacji w zakresie ochrony danych osobowych, którego ogólny zakres oparto na kryteriach natury ogólnej:

a) Bezpieczne logowanie

Bezpieczne logowanie stanowi operację przetwarzania zrozumiałą dla użytkownika końcowego i istotną z punktu widzenia ochrony danych, ponieważ odgrywa istotną rolę w zapewnianiu bezpieczeństwa danych osobowych. W związku z tym prowadzenie tej operacji przetwarzania jest konieczne na potrzeby bezpiecznego logowania, a zatem może stanowić znaczący przedmiot oceny, jeżeli z certyfikatu jasno wynika, że certyfikuje się wyłącznie operację przetwarzania logowania.

b) Front-end strony internetowej

Chociaż front-end strony internetowej może być istotny z punktu widzenia ochrony danych osobowych, nie jest on zrozumiały dla użytkownika końcowego, a zatem nie może stanowić znaczącego przedmiotu oceny. Ponadto dla użytkownika nie jest jasne, jakie usługi na stronie internetowej (a zatem jakie operacje przetwarzania) obejmuje certyfikacja.

c) Elektroniczne usługi bankowe

Front-end i back-end strony internetowej to operacje przetwarzania wykorzystywane w ramach elektronicznych usług bankowych, które mogą mieć znaczenie dla użytkownika. W tym kontekście oba te elementy muszą być objęte przedmiotem oceny. Z przedmiotu oceny można wyłączyć operacje przetwarzania, które nie są bezpośrednio związane ze świadczeniem elektronicznych usług bankowych, takie jak operacje przetwarzania mające na celu zapobieganie praniu pieniędzy.

Elektroniczne usługi bankowe oferowane przez bank za pośrednictwem jego strony internetowej mogą jednak również obejmować inne usługi, które z kolei wymagają prowadzenia osobnych operacji przetwarzania. W tym kontekście inne usługi mogą obejmować na przykład oferowanie produktu ubezpieczeniowego. Ponieważ ta dodatkowa usługa nie jest bezpośrednio związana z celem świadczenia elektronicznych usług bankowych, można ją wyłączyć z przedmiotu oceny. Jeżeli ta dodatkowa usługa (ubezpieczenie) jest wyłączona z przedmiotu oceny, interfejsy dla tej usługi zintegrowane ze stroną internetową są częścią przedmiotu oceny, w związku z czym należy je opisać w celu dokonania wyraźnego rozróżnienia między usługami. Sporządzenie takiego opisu jest konieczne do określenia i oceny potencjalnych przepływów danych między tymi dwoma usługami.

60. [Przykład 2]

    Bank oferuje klientom usługę umożliwiającą agregację informacji związanych z poszczególnymi rachunkami i kartami kredytowymi pochodzącymi z kilku banków (agregacja rachunków). Bank pragnie certyfikować tę usługę na podstawie RODO. Właściwy organ nadzorczy zatwierdził konkretny zestaw kryteriów certyfikacji dotyczących tego rodzaju działalności. Zakres mechanizmu certyfikacji dotyczy wyłącznie następujących aspektów zgodności:

    - uwierzytelnienie użytkownika; a także
    - akceptowalne sposoby pozyskiwania danych, które mają być agregowane, z innych banków/usług.

    Ponieważ zakres stosowania tego mechanizmu certyfikacji sam w sobie określa przedmiot oceny, nie jest możliwe znaczące zawężenie tego przedmiotu oceny w proponowanym zakresie i certyfikacja jedynie szczególnych cech lub pojedynczej czynności przetwarzania. W takim wypadku przedmiot oceny musi być równy określonemu zakresowi.

5.3 Metody ewaluacji i metodyka oceny

61. Ocena zgodności umożliwiająca wykazanie zgodności operacji przetwarzania wymaga zidentyfikowania i określenia metod ewaluacji i metodyki oceny. Istotne jest to, czy informacje wykorzystywane do oceny czerpie się wyłącznie z dokumentacji (która sama w sobie mogłaby być niewystarczająca), czy też czynnie gromadzi się je na miejscu oraz w drodze bezpośredniego lub pośredniego dostępu. Sposób gromadzenia informacji wpływa na znaczenie certyfikacji i w związku z tym należy go określić i opisać.

    Procedury udzielania i okresowego przeglądu certyfikacji powinny obejmować specyfikacje umożliwiające określenie właściwego poziomu ewaluacji (zakresu i szczegółowości) w celu spełnienia kryteriów certyfikacji. Powinny one także obejmować:

    - udzielenie informacji i przedstawienie specyfikacji zastosowanych metod oceny i ustaleń powziętych np. podczas audytów na miejscu lub pozyskanych z dokumentacji;

- przedstawienie metod ewaluacji skupiających się na operacjach przetwarzania (danych, systemów, procesów) i celu tego przetwarzania;
- określenie kategorii danych, potrzeb w zakresie ochrony oraz tego, czy zaangażowane są podmioty przetwarzające lub osoby trzecie;
- określenie ról oraz istnienia mechanizmu kontroli dostępu zdefiniowanego w odniesieniu do ról i obowiązków.

62. Zakres ewaluacji wpływa na znaczenie i wartość certyfikacji. Ograniczenie zakresu ewaluacji do celów pragmatycznych lub z myślą o obniżeniu kosztów zmniejszy znaczenie certyfikacji w zakresie ochrony danych osobowych. Z kolei decyzje dotyczące szczegółowości ewaluacji mogą przekraczać możliwości finansowe wnioskodawcy, a także często zdolność oceniających i audytorów. W celu wykazania zgodności nie zawsze kluczowe jest przeprowadzenie bardzo szczegółowej analizy wykorzystywanych systemów informatycznych, aby certyfikacja pozostała znacząca.

5.4 Dokumentacja oceny

63. Dokumentacja certyfikacyjna powinna być dokładna i wszechstronna. Brak dokumentacji oznacza, że nie można przeprowadzić właściwej oceny. Podstawową funkcją dokumentacji certyfikacyjnej jest zapewnienie przejrzystości procesu oceny w ramach mechanizmu certyfikacji. Dokumentacja dostarcza odpowiedzi na pytania dotyczące wymogów określonych w przepisach prawa. Mechanizmy certyfikacji powinny przewidywać znormalizowaną metodologię dokumentacji. W następnej kolejności ocena umożliwi porównanie dokumentacji certyfikacyjnej ze stanem faktycznym na miejscu oraz z kryteriami certyfikacji.

64. Wyczerpująca dokumentacja dotycząca tego, co już certyfikowano, oraz zastosowanej metodyki służy do zapewnienia przejrzystości. Zgodnie z art. 43 ust. 2 lit. c) mechanizmy certyfikacji powinny określać procedury umożliwiające dokonanie przeglądu certyfikacji. Aby umożliwić organowi nadzorczemu ocenę, czy i w jakim zakresie certyfikację można potwierdzić w toku formalnych postępowań wyjaśniających, szczegółowa dokumentacja może okazać się najodpowiedniejszym środkiem komunikacji. W dokumentacji przedstawionej podczas oceny należy zatem skupić się na trzech głównych aspektach:
    - zgodności i spójności stosowanych metod oceny;
    - metodach oceny mających na celu wykazanie zgodności przedmiotu certyfikacji z kryteriami certyfikacji, a zatem z rozporządzeniem; a także
    - wykazaniu, że wyniki ewaluacji zatwierdził niezależny i bezstronny podmiot certyfikujący.

5.5 Dokumentacja wyników

65. W motywie 100 przedstawiono informacje na temat celów związanych z wprowadzeniem certyfikacji.

„Aby zwiększyć przejrzystość i poprawić przestrzeganie niniejszego rozporządzenia, należy zachęcać do ustanowienia mechanizmów certyfikacji oraz do wprowadzenia znaków jakości i oznaczeń w dziedzinie ochrony danych, pozwalając w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi."

66. W zwiększaniu przejrzystości istotną rolę odgrywa dokumentacja i informowanie o wynikach. Podmioty certyfikujące wykorzystujące mechanizmy certyfikacji, znaki jakości i oznaczenia skierowane do osób, których dane dotyczą (pełniących role konsumentów lub klientów) powinny zapewniać łatwo dostępne, zrozumiałe i stosowne informacje na temat certyfikowanych operacji przetwarzania. Te informacje publiczne powinny obejmować co najmniej:

    - opis przedmiotu oceny;
    - odniesienie do zatwierdzonych kryteriów mających zastosowanie do konkretnego przedmiotu oceny;
    - metodykę ewaluacji kryteriów (ewaluacja na miejscu, dokumentacja itd.); a także
    - okres ważności certyfikatu; a także
    - powinny zapewniać organom nadzorczym i opinii publicznej porównywalność wyników.

6 WYTYCZNE DOTYCZĄCE OKREŚLANIA KRYTERIÓW CERTYFIKACJI

67. Kryteria certyfikacji stanowią integralną część mechanizmu certyfikacji. Procedura certyfikacji obejmuje wymogi przewidujące, kto, w jaki sposób, w jakim stopniu i z jaką szczegółowością przeprowadza ocenę, która odbywa się w ramach poszczególnych projektów certyfikacyjnych dotyczących konkretnego przedmiotu oceny. Kryteria certyfikacji określają wymogi nominalne, w odniesieniu do których ocenia się rzeczywiste operacje przetwarzania zdefiniowane w ramach przedmiotu oceny. W niniejszych wytycznych dotyczących określania kryteriów certyfikacji przedstawiono ogólne wskazówki ułatwiające prowadzenie oceny kryteriów certyfikacji do celów zatwierdzenia.

    - Przy zatwierdzaniu lub określaniu kryteriów certyfikacji należy wziąć pod uwagę następujące kwestie ogólne. Kryteria certyfikacji powinny:
    - być jednorodne i możliwe do zweryfikowania;
    - być możliwe do skontrolowania w celu ułatwienia prowadzenia ewaluacji operacji przetwarzania na podstawie RODO, w szczególności poprzez określenie celów i wytycznych wykonawczych służących osiąganiu tych celów;
    - być adekwatne w odniesieniu do odbiorców docelowych (np. w relacjach B2B i między przedsiębiorstwami a konsumentami (B2C));

- uwzględniać inne normy (takie jak normy ISO, normy krajowe) i w stosownych przypadkach być z nimi interoperacyjne; a także
- być elastyczne i skalowalne w celu umożliwienia zastosowania do organizacji różnych rodzajów i rozmiarów, m.in. mikro, małych i średnich przedsiębiorstw zgodnie z art. 42 ust. 1 oraz stosowania podejścia opartego na analizie ryzyka zgodnie z motywem 77.

68. Małe przedsiębiorstwo lokalne, takie jak sprzedawca detaliczny, prowadzi zazwyczaj mniej skomplikowane operacje przetwarzania niż duży, wielonarodowy sprzedawca detaliczny. Chociaż wymogi dotyczące zgodności z prawem operacji przetwarzania są takie same, należy uwzględnić zakres przetwarzania danych i złożoność procesu przetwarzania; wynika z tego, że istnieje potrzeba, aby mechanizmy certyfikacji i ich kryteria były skalowalne w zależności od danej czynności przetwarzania.

6.1 Istniejące normy

69. Podmioty certyfikujące będą musiały rozważyć, w jaki sposób w konkretnych kryteriach uwzględnia się istniejące stosowne instrumenty, takie jak kodeksy postępowania, normy techniczne lub krajowe inicjatywy regulacyjne i prawne. Najlepiej byłoby, gdyby kryteria charakteryzowały się interoperacyjnością z istniejącymi normami mogącymi pomóc administratorowi lub podmiotowi przetwarzającemu wypełniać swoje obowiązki wynikające z RODO. Chociaż normy branżowe często skupiają się na ochronie organizacji przed zagrożeniami i ich bezpieczeństwie, RODO jest jednak ukierunkowane na ochronę praw podstawowych osób fizycznych. Przy opracowywaniu lub zatwierdzaniu kryteriów lub mechanizmów certyfikacji opartych na normach branżowych należy uwzględnić tę odmienną perspektywę.

6.2 Określenie kryteriów

70. Kryteria certyfikacji muszą odpowiadać stwierdzeniu zawartemu w certyfikacie (komunikatowi lub roszczeniu) dotyczącemu mechanizmu lub systemu certyfikacji i muszą być zgodne z oczekiwaniami, jakie ono wzbudza. Już sama nazwa mechanizmu certyfikacji może określać zakres stosowania i będzie mieć konsekwencje dla określenia kryteriów.

71. [Przykład 3]

    Mechanizm o nazwie „HealthPrivacyMark” powinien mieć zakres ograniczony do sektora zdrowia. Nazwa znaku jakości wzbudza oczekiwanie, że wymogi w zakresie ochrony danych osobowych zbadano w połączeniu z danymi dotyczącymi zdrowia. W związku z tym kryteria stosowane w ramach tego mechanizmu muszą być odpowiednie do celów oceny wymogów w zakresie ochrony danych osobowych w tym sektorze.

72. [Przykład 4]

Mechanizm, który odnosi się do certyfikacji operacji przetwarzania obejmujących systemy zarządzania przetwarzaniem danych, powinien określać kryteria pozwalające na rozpoznanie i ocenę procesów zarządzania i wspierających je środków technicznych i organizacyjnych.

73. [Przykład 5]

    Kryteria dotyczące mechanizmu, który odnosi się do przetwarzania w chmurze, muszą uwzględniać specjalne wymogi techniczne niezbędne do korzystania z usług w chmurze. Przykładowo, jeżeli wykorzystywane są serwery poza UE, kryteria muszą uwzględniać warunki określone w rozdziale V RODO w odniesieniu do przekazywania danych do państw trzecich.

74. Kryteria, które mają dotyczyć różnych przedmiotów oceny w różnych sektorach lub państwach członkowskich, powinny: umożliwiać stosowanie różnych scenariuszy; umożliwiać określanie odpowiednich środków w celu dostosowania kryteriów do małych, średnich lub dużych operacji przetwarzania i odzwierciedlać zagrożenia związane z różnym prawdopodobieństwem i wagą zagrożeń dotyczących praw i wolności osób fizycznych zgodnie z RODO. W związku z tym procedury certyfikacyjne (np. w odniesieniu do dokumentacji, badania lub zakresu i metod ewaluacji), które uzupełniają kryteria, muszą odpowiadać tym potrzebom oraz umożliwiać oraz przewidywać wprowadzenie zasad, przewidujących na przykład stosowanie odpowiednich kryteriów w poszczególnych projektach certyfikacyjnych. Kryteria muszą ułatwić przeprowadzenie oceny dotyczącej tego, czy wdrożenie odpowiednich środków technicznych i organizacyjnych zagwarantowano w wystarczającym stopniu.

6.3 Okres ważności kryteriów certyfikacji

75. Chociaż kryteria certyfikacji muszą pozostawać wiarygodne z upływem czasu, powinno się zachować w odniesieniu do nich możliwość zmiany. Podlegają one przeglądowi na przykład w sytuacji, gdy:

    - zmianie ulegną ramy prawne;
    - Trybunał Sprawiedliwości dokona w swoich orzeczeniach wykładni warunków i przepisów; lub
    - zmieni się aktualny stan wiedzy technicznej.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

ZAŁĄCZNIK 1: ZADANIA I UPRAWNIENIA ORGANÓW NADZORCZYCH W ODNIESIENIU DO CERTYFIKACJI NA PODSTAWIE RODO.

	Przepisy	Wymogi
Zadania	Art. 43 ust. 6	Zobowiązuje organ nadzorczy do podania do wiadomości publicznej kryteriów, o których mowa w art. 42 ust. 5, w łatwo dostępny sposób oraz do przekazania tych kryteriów Europejskiej Radzie Ochrony Danych.
	Art. 57 ust. 1 lit. n)	Zobowiązuje organ nadzorczy do zatwierdzania kryteriów certyfikacji zgodnie z art. 42 ust. 5.
	Art. 57 ust. 1 lit. o)	Zapewnia, że gdy ma to zastosowanie (tj. gdy organ udziela certyfikacji), dokonuje on okresowego przeglądu udzielonych certyfikacji zgodnie z art. 42 ust. 7.
	Art. 64 ust. 1 lit. c)	Zobowiązuje organ nadzorczy do zgłoszenia Europejskiej Radzie Ochrony Danych projektu decyzji, w przypadku gdy zamierza zatwierdzić kryteria certyfikacji, o których mowa w art. 42 ust. 5.
Uprawnienia	Art. 58 ust. 1 lit. c)	Uprawnia organ nadzorczy do dokonywania przeglądu udzielonych certyfikacji na podstawie art. 42 ust. 7.
	Art. 58 ust. 2 lit. h)	Uprawnia organ nadzorczy do cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu cofnięcia certyfikacji, lub nakazania podmiotowi certyfikującemu nieudzielania certyfikacji.
	Art. 58 ust. 3 lit. e)	Uprawnia organ nadzorczy do akredytowania podmiotów certyfikujących.
	Art. 58 ust. 3 lit. f)	Uprawnia organ nadzorczy do udzielania certyfikacji i zatwierdzanie kryteriów certyfikacji.
	Art. 58 ust. 3 lit. e)	Uprawnia organ nadzorczy do akredytowania podmiotów certyfikujących.
	Art. 58 ust. 3 lit. f)	Uprawnia organ nadzorczy do udzielania certyfikacji i zatwierdzanie kryteriów certyfikacji.

ZAŁĄCZNIK 2

1 WPROWADZENIE

Załącznik 2 zawiera wytyczne dotyczące przeglądu i oceny kryteriów certyfikacji zgodnie z art. 42 ust. 5. W załączniku zidentyfikowano zagadnienia, które organy nadzorcze ds. ochrony danych oraz EROD wezmą pod uwagę i zastosują podczas zatwierdzania kryteriów certyfikacji dla mechanizmu certyfikacji. Pytania powinny być rozpatrywane przez podmioty certyfikujące i właścicieli systemów, którzy chcą opracować i przedstawiać kryteria zatwierdzania. Wykaz ten nie jest wyczerpujący, ale przedstawia minimum zagadnień, które należy wziąć pod uwagę. Nie wszystkie pytania będą miały zastosowanie; należy je jednak uwzględnić przy opracowywaniu kryteriów i uzasadnienia, aby wyjaśnić, dlaczego kryteria nie obejmują określonych aspektów. Niektóre pytania powtarzają się, ponieważ są zadawane w ramach różnych perspektyw. Niniejsze wytyczne należy rozpatrywać zgodnie z wymogami prawnymi przewidzianymi w RODO oraz, w stosownych przypadkach, w ustawodawstwie krajowym.

2 ZAKRES MECHANIZMU CERTYFIKACJI I PRZEDMIOT OCENY

a. Czy jasno opisano zakres mechanizmu certyfikacji (w odniesieniu do którego stosuje się kryteria ochrony danych)?

b. Czy zakres mechanizmu certyfikacji ma znaczenie dla grupy odbiorców, do której jest skierowany? Czy może wprowadzać w błąd?

- *Na przykład: Znak jakości „zaufane przedsiębiorstwo" sugeruje, że przeprowadzono kontrolę działalności w odniesieniu do całego przedsiębiorstwa, chociaż jedynie określone operacje przetwarzania danych, np. proces płatności online, faktycznie podlegają certyfikacji. W związku z tym zakres jest mylący.*

c. Czy zakres mechanizmu certyfikacji odzwierciedla wszystkie istotne aspekty operacji przetwarzania?

- *Na przykład: Znak jakości „poszanowanie życia prywatnego w dziedzinie zdrowia" musi obejmować wszystkie dane dotyczące stanu zdrowia w celu spełnienia wymogów określonych w art. 9.*

d. Czy zakres mechanizmu certyfikacji umożliwia znaczące poświadczenie ochrony danych, biorąc pod uwagę charakter, treść oraz ryzyko związane z operacjami przetwarzania?

- *Na przykład: Jeżeli zakres mechanizmu certyfikacji koncentruje się wyłącznie na określonych aspektach operacji przetwarzania danych, takich jak gromadzenie danych, ale nie na dalszych operacjach przetwarzania, takich jak przetwarzanie w celu tworzenia profili reklamowych lub zarządzanie prawami osób, których dane dotyczą, to nie jest on znaczący dla osób, których dane dotyczą.*

e. Czy zakres mechanizmu certyfikacji obejmuje przetwarzanie danych osobowych w odpowiednim kraju, w którym złożono wniosek, czy też dotyczy przetwarzania i/lub przenoszenia transgranicznego?

f. Czy kryteria certyfikacji w wystarczającym stopniu opisują sposób definiowania przedmiotu oceny?

- *Na przykład: „Marka ochrony danych osobowych" o zakresie ogólnym, która wymagałaby jedynie „specyfikacji przetwarzania będącego przedmiotem certyfikacji", nie zawierałaby wystarczająco jasnych wskazówek na temat sposobu ustalania i opisywania przedmiotu oceny.*
- *Na przykład: Szczegółowy zakres, „znaku jakości ochrony życia prywatnego dla sejfów cyfrowych" dotyczącego bezpiecznego przechowywania danych powinien szczegółowo opisywać wymogi dotyczące spełnienia tego zakresu w swoich kryteriach, np. definicję sejfu cyfrowego, wymogi dotyczące systemu oraz obowiązkowe środki techniczne i organizacyjne. W takim przypadku możliwe jest wyraźne zdefiniowanie przedmiotu oceny.*

    1) Czy kryteria wymagają, aby przedmiot oceny zawierał identyfikację wszystkich istotnych operacji przetwarzania, przedstawienie przepływów danych oraz określenie obszaru zastosowania przedmiotu oceny?

        - *Na przykład: Mechanizm certyfikacji zapewnia certyfikację operacji przetwarzania danych przez administratorów danych w ramach RODO, ale nie określa obszaru zastosowania (zakres ogólny). Kryteria stosowane w ramach mechanizmu wymagają od administratora ubiegającego się o certyfikację określenia operacji przetwarzania danych (przedmiotu oceny) w odniesieniu do stosowanych rodzajów danych, systemów i procesów.*

    2) Czy kryteria wymagają od wnioskodawcy wyraźnego określenia, gdzie przetwarzanie, które podlega ocenie, rozpoczyna się i kończy? Czy kryteria wymagają, aby przedmiot oceny zawierał interfejsy, w przypadku których współzależne czynności przetwarzania nie są uwzględnione jako część przedmiotu oceny? I czy jest to należycie uzasadnione?

        - *Na przykład: Przedmiot oceny opisujący w sposób wystarczająco szczegółowy proces przetwarzania usługi sieciowej, takiej jak rejestracja użytkowników, świadczenie usług, fakturowanie, rejestrowanie adresów IP, interfejsy z użytkownikami oraz stronami trzecimi, z wyłączeniem hostingu serwerów (ale włączając umowy w sprawie przetwarzania oraz środków technicznych i organizacyjnych).*

g. Czy kryteria gwarantują, że poszczególne przedmioty oceny są zrozumiałe dla odbiorców, w tym w stosownych przypadkach osób, których dane dotyczą?

3 WYMOGI OGÓLNE

a. Czy wszystkie terminy stosowane w katalogu kryteriów (tj. pełny zestaw kryteriów certyfikacji) zostały określone, wyjaśnione i opisane?

b. Czy zidentyfikowano wszystkie odniesienia normatywne?

c. Czy kryteria obejmują definicję obowiązków, procedur i operacji przetwarzania w zakresie ochrony danych objętych zakresem stosowania mechanizmu certyfikacji?

4 OPERACJA PRZETWARZANIA, ART. 42 UST. 1

W odniesieniu do zakresu mechanizmu certyfikacji (ogólnego lub szczególnego), czy wszystkie istotne elementy operacji przetwarzania danych (dane, systemy i procesy) zostały uwzględnione w kryteriach?

a. Czy kryteria wymagają zidentyfikowania ważnych podstaw prawnych przetwarzania danych w odniesieniu do przedmiotu oceny?

b. Czy, w odniesieniu do przedmiotu oceny, kryteria uwzględniają odpowiednie fazy przetwarzania danych i cały cykl życia danych, w tym ich usunięcie i anonimizację?

c. Czy, w odniesieniu do przedmiotu oceny, kryteria wymagają możliwości przenoszenia danych?

d. Czy, w odniesieniu do przedmiotu oceny, kryteria pozwalają na zidentyfikowanie i odzwierciedlenie szczególnych rodzajów operacji przetwarzania danych, np. automatycznego podejmowania decyzji, profilowania?

e. Czy, w odniesieniu do przedmiotu oceny, kryteria pozwalają na określenie szczególnych kategorii danych?

f. Czy kryteria przewidują (wymagają) oceny ryzyka poszczególnych operacji przetwarzania oraz potrzeb w zakresie ochrony praw i wolności osób, których dane dotyczą?

g. Czy kryteria przewidują (wymagają) odpowiednie uwzględnienie zagrożeń dla praw i wolności osób fizycznych?

…

5 ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

a. Czy kryteria wymagają sprawdzenia zgodności z prawem przetwarzania danych dla poszczególnych operacji przetwarzania w odniesieniu do celu i konieczności przetwarzania?

b. Czy kryteria wymagają sprawdzenia wszystkich wymogów podstawy prawnej dla poszczególnych operacji przetwarzania?

6 ZASADY, ART. 5

a. Czy kryteria uwzględniają w odpowiedni sposób wszystkie zasady ochrony danych zgodnie z art. 5?

b. Czy kryteria wymagają wykazania poszanowania zasady minimalizacji danych dla poszczególnych przedmiotów oceny?

…

7 OGÓLNE OBOWIĄZKI ADMINISTRATORÓW I PODMIOTÓW PRZETWARZAJĄCYCH

a. Czy kryteria wymagają potwierdzenia porozumień umownych między podmiotami przetwarzającymi a administratorami danych?

b. Czy umowy między podmiotami przetwarzającymi a administratorami danych są przedmiotem oceny?

c. Czy kryteria odzwierciedlają obowiązki administratora wynikające z rozdziału IV?

d. Czy kryteria wymagają dowodu dokonania przeglądu i aktualizacji środków technicznych i organizacyjnych wprowadzonych przez administratora zgodnie z art. 24 ust. 1?

e. Czy kryteria obejmują sprawdzenie, czy organizacja dokonała oceny stosowności wyznaczenia inspektora ochrony danych zgodnie z wymogami art. 37? W stosownych przypadkach czy inspektor ochrony danych spełnia wymogi określone w art. 37 – 39?

f. Czy kryteria obejmują sprawdzenie, czy rejestry czynności przetwarzania danych są wymagane zgodnie z art. 30 ust. 5 i w odpowiedni sposób uwzględniają wymogi określone w art. 30?

8 PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

a. Czy kryteria w odpowiedni sposób odnoszą się do prawa osób, których dane dotyczą, do informacji oraz wymagają wprowadzenia odpowiednich środków?

b. Czy kryteria wymagają, aby osobom, których dane dotyczą, przyznano odpowiedni, a nawet wyższy poziom dostępu i kontroli do ich danych, w tym możliwość przenoszenia danych?

c. Czy kryteria wymagają wprowadzenia środków przewidujących możliwość interwencji w ramach operacji przetwarzania w celu zagwarantowania praw osób, których dane dotyczą, oraz umożliwienia wprowadzania korekt, ograniczeń lub usuwania danych?

…

9 RYZYKO NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH

a. Czy kryteria przewidują (wymagają) dokonanie oceny zagrożeń dla praw i wolności osób fizycznych?

b. Czy kryteria przewidują lub wymagają zastosowania uznanej metodyki oceny ryzyka? W stosownych przypadkach, czy jest to współmierne?

c. Czy kryteria przewidują (wymagają) dokonanie oceny wpływu przewidywanych operacji przetwarzania na prawa i wolności osób fizycznych?

d. Czy kryteria wymagają uprzedniej konsultacji w sprawie pozostałych czynników ryzyka, które nie mogłyby zostać ograniczone na podstawie wyników oceny skutków dla ochrony danych?

10 ŚRODKI TECHNICZNE I ORGANIZACYJNE GWARANTUJĄCE OCHRONĘ

a. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych zapewniających poufność operacji przetwarzania?

b. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych zapewniających integralność operacji przetwarzania?

c. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych zapewniających dostępność operacji przetwarzania?

d. Czy kryteria wymagają zastosowania środków zapewniających przejrzystość operacji przetwarzania w odniesieniu do:

e. rozliczalności?

f. praw osób, których dane dotyczą?

g. oceny poszczególnych operacji przetwarzania, np. w odniesieniu do przejrzystości algorytmów?

h. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych gwarantujących prawa osób, których dane dotyczą, np. możliwości dostarczania informacji lub przenoszenia danych?

i. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych zapewniających możliwość interwencji w ramach operacji przetwarzania w celu zagwarantowania praw osób, których dane dotyczą, oraz umożliwienia wprowadzania korekt, ograniczeń lub usuwania danych?

j. Czy kryteria wymagają zastosowania środków zapewniających możliwość interwencji w ramach operacji przetwarzania w celu w celu naprawienia lub sprawdzenia systemu lub procesu?

k. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych w celu zapewnienia minimalizacji danych, na przykład niełączenia lub oddzielenia danych od podmiotu danych, anonimizacji lub pseudonimizacji lub izolacji systemów danych?

l. Czy kryteria wymagają zastosowania środków technicznych w celu wdrożenia domyślnej ochrony danych?

m. Czy kryteria wymagają środków technicznych i organizacyjnych wdrażających ochronę danych już w fazie projektowania, np. system zarządzania ochroną danych w celu wykazania, kontroli i egzekwowania wymogów ochrony danych oraz informowania o nich?

n. Czy kryteria wymagają środków technicznych i organizacyjnych wdrażających odpowiednie okresowe szkolenia dla personelu mającego stały lub regularny dostęp do danych osobowych?

o. Czy kryteria wymagają przeglądu środków?

p. Czy kryteria wymagają samooceny/audytu wewnętrznego?

q. Czy kryteria wymagają zastosowania środków w celu zapewnienia, by obowiązki w zakresie powiadamiania o naruszeniu ochrony danych osobowych były wykonywane w odpowiednim czasie i zakresie?

r. Czy kryteria wymagają wprowadzenia i weryfikacji procedur zarządzania incydentami?

s. Czy kryteria wymagają monitorowania zmian związanych z prywatnością i technologią oraz aktualizacji programu w razie potrzeby?

…

11 INNE CECHY SZCZEGÓLNE SPRZYJAJĄCE OCHRONIE DANYCH

a. Czy kryteria wymagają wdrożenia technik służących poprawie ochrony danych? Może to obejmować kryteria, które wymagają zwiększonej ochrony danych poprzez wyeliminowanie lub ograniczenie danych osobowych, lub czynniki ryzyka dla ochrony danych.

- *Na przykład: Kryteria wymagające większego stopnia niepołączalności danych poprzez wykorzystanie rozwiązań zarządzania tożsamością zorientowanych na użytkownika, takich jak dane uwierzytelniające oparte na atrybutach (ABC), zamiast rozwiązań*

zarządzania tożsamością zorientowanych na organizację, odzwierciedlałyby technikę wzmacniającą ochronę danych.

b. Czy kryteria wymagają wdrożenia wzmocnionych kontroli ze strony osób, których dane dotyczą w celu ułatwienia samostanowienia i wyboru?

…

12 KRYTERIA SŁUŻĄCE WYKAZANIU ISTNIENIA ODPOWIEDNICH ZABEZPIECZEŃ W ODNIESIENIU DO PRZEKAZYWANIA DANYCH OSOBOWYCH

Kryteria zostaną uwzględnione w przyszłych wytycznych w sprawie art. 42 ust. 2.

13 DODATKOWE KRYTERIA DOTYCZĄCE EUROPEJSKIEGO ZNAKU JAKOŚCI OCHRONY DANYCH

a. Czy kryteria obejmują wszystkie państwa członkowskie?

b. Czy kryteria umożliwiają uwzględnienie przepisów lub scenariuszy danego państw członkowskich dotyczących ochrony danych?

c. Czy kryteria wymagają dokonania oceny poszczególnych przedmiotów oceny w odniesieniu do przepisów dotyczących ochrony danych obowiązujących w danym sektorze w danym państwie członkowskim?

d. Czy kryteria wymagają od administratora lub podmiotu przetwarzającego dostarczania informacji osobom, których dane dotyczą, oraz zainteresowanym stronom, w językach państw członkowskich:

e. informacje w sprawie przetwarzania/przedmiotu oceny?

f. dokumentacja dotycząca przetwarzania/przedmiotu oceny?

g. wyniki oceny?

…

14 OGÓLNA OCENA KRYTERIÓW

a. Czy kryteria w pełni obejmują zakres mechanizmu certyfikacji (tj. kryteria kompleksowe), zapewniając tym samym wystarczające gwarancje, aby można było zaufać certyfikacji?

- *Na przykład: Jeżeli zakres mechanizmu certyfikacji koncentruje się na operacjach przetwarzania danych dotyczących zdrowia, należy zagwarantować wysoki poziom ochrony danych, określając kryteria zapewniające np. pogłębioną ocenę i stosowanie zasad ochrony prywatności już w fazie projektowania oraz domyślnej prywatności.*

b. Czy kryteria są proporcjonalne do rozmiaru czynności przetwarzania objętych zakresem mechanizmu certyfikacji, do wrażliwość informacji i do ryzyka związanego z przetwarzaniem?

c. Czy kryteria mogą poprawić przestrzeganie przepisów dotyczących ochrony danych przez administratorów i podmioty przetwarzające?

d. Czy osoby, których dane dotyczą, będą mogły korzystać z przysługujących im praw do informacji, w tym z objaśnienia im pożądanych wyników?