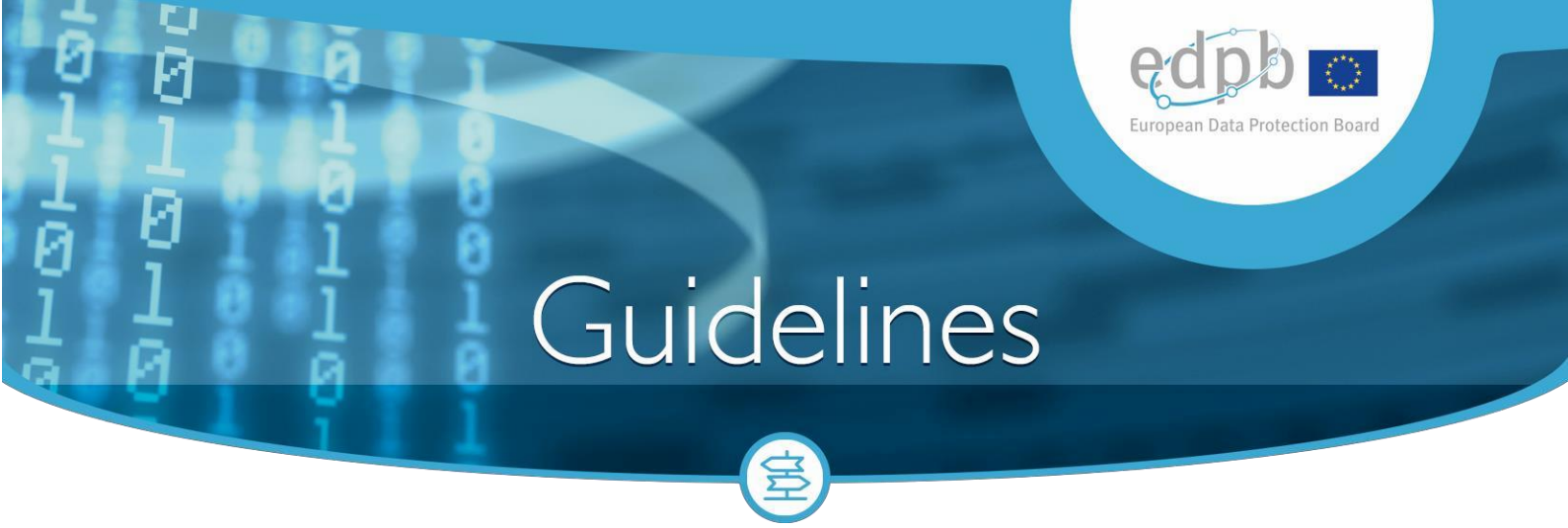

Wytyczne 1/2018 dotyczące certyfikacji i określania kryteriów certyfikacji zgodnie z artykułami 42 i 43 rozporządzenia 2016/679

Przyjęte 25 maja 2018 r.

Spis treści

1. Wprowadzenie 2
1.1. Zakres wytycznych 3
1.2. Cel certyfikacji na mocy RODO 4
1.3. Kluczowe pojęcia 5
1.3.1. Interpretacja „certyfikacji” 5
1.3.2. Mechanizmy certyfikacji, znaki jakości i oznaczenia 5
2. Rola organów nadzorczych 5
2.1 Organ nadzorczy jako podmiot certyfikujący 6
2.2 Dalsze zadania organu nadzorczego odnośnie certyfikacji 6
3. Rola podmiotu certyfikującego 7
4. Zatwierdzanie kryteriów certyfikacji 8
4.1. Termin zatwierdzenia 8
4.2. Właściwy organ nadzorczy 8
4.3. Europejski znak jakości ochrony danych 9
5. Opracowanie kryteriów certyfikacji 9
5.1. Co może być objęte certyfikacją na mocy RODO? 10
5.2. Określanie przedmiotu certyfikacji 11
5.3. Metody ewaluacji i metodologia oceny 13
5.4. Dokumentacja oceny 14
5.5. Dokumentacja wyników 14
6. Wytyczne dotyczące określania kryteriów certyfikacji 14
6.1. Istniejące standardy 15
6.2. Określanie kryteriów 15
6.3. Okres ważności kryteriów certyfikacji 16
Załącznik: Zadania i prawa organów nadzorczych odnośnie certyfikacji zgodnie z RODO 17

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia 2016/679/UE Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, uchylającego dyrektywę 95/46/WE,

PRZYJĘŁA PONIŻSZE WYTYCZNE:

1. Wprowadzenie

Ogólne rozporządzenie o ochronie danych (rozporządzenie 2016/279, „RODO" lub „rozporządzenie") określa zmodernizowane ramy rozliczalności i poszanowania praw podstawowych w zakresie ochrony danych w Europie. Kluczowe znaczenie dla tych nowych ram ma szereg środków ułatwiających przestrzeganie zapisów RODO. Obejmują one wymogi obowiązkowe w określonych okolicznościach (w tym mianowanie inspektorów ochrony danych i przeprowadzanie ocen skutków dla ochrony danych) oraz środki dobrowolne, takie jak kodeksy postępowania i mechanizmy certyfikacji.

Przed przyjęciem RODO GR Art. 29 ustaliła, że certyfikacja może odgrywać istotną rolę w ramach rozliczalności w zakresie ochrony danych.[1] Aby certyfikacja zapewniała wiarygodne dowody zgodności z zasadami ochrony danych, konieczne są jasne zasady określające wymogi dotyczące certyfikacji.[2] Artykuł 42 RODO stanowi podstawę prawną dla opracowania takich zasad.

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."*

Mechanizmy certyfikacji[3] mogą poprawić przejrzystość w odniesieniu do osób fizycznych, ale również w relacjach między przedsiębiorstwami, na przykład między administratorami i podmiotami przetwarzającymi. Motyw 100 RODO stanowi, że ustanowienie mechanizmów certyfikacji może zwiększyć przejrzystość i poprawić przestrzeganie rozporządzenia oraz zezwolić poszczególnym osobom fizycznym na ocenę poziomu ochrony danych, której podlegają stosowne produkty i usługi.[4]

[1] Grupa Robocza Art. 29, Opinia 3/2010 w sprawie zasady rozliczalności (WP173), 13 lipca 2010, punkty 69-71.
[2] Grupa Robocza Art. 29, Opinia 3/2010 w sprawie zasady rozliczalności (WP173), punkt 69.
[3] W niniejszych wytycznych mechanizmy certyfikacji oraz znaki jakości i oznaczenia dotyczące ochrony danych zbiorczo zwane są „mechanizmami certyfikacji", zob. część 1.3.2.
[4] Motyw 100 RODO stanowi, że „aby zwiększyć przejrzystość i poprawić przestrzeganie niniejszego rozporządzenia, należy zachęcać do ustanowienia mechanizmów certyfikacji (...), pozwalając w ten sposób osobom, których dane dotyczą, szybko

RODO nie wprowadza prawa ani obowiązku certyfikacji dla administratorów i podmiotów przetwarzających. Zgodnie z art. 42 ust. 3 certyfikacja jest dobrowolnym procesem mającym na celu pomoc w wykazaniu zgodności z RODO. Państwa członkowskie i organy nadzorcze powinny zachęcać do ustanowienia mechanizmów certyfikacji i określą formy zaangażowania zainteresowanych stron w proces i cykl certyfikacji.

Ponadto przestrzeganie zatwierdzonych mechanizmów certyfikacji jest czynnikiem, który organy nadzorcze muszą brać pod uwagę jako czynnik obciążający lub łagodzący przy podejmowaniu decyzji o nałożeniu administracyjnej kary pieniężnej i przy podejmowaniu decyzji w sprawie kwoty takiej kary (art. 83 ust. 2 lit. j))[5].

1.1. Zakres wytycznych

Niniejsze wytyczne mają ograniczony zakres. Nie stanowią one podręcznika postępowania służącego do certyfikacji zgodnie z RODO. Głównym celem niniejszych wytycznych jest określenie nadrzędnych kryteriów, które mogą być istotne dla wszystkich rodzajów mechanizmów certyfikacji wydanych zgodnie z art. 42 i 43 RODO. W tym celu niniejsze wytyczne:

- zgłębiają podstawy certyfikacji jako narzędzia rozliczalności;
- wyjaśniają kluczowe pojęcia przepisów dotyczących certyfikacji zawartych w art. 42 i 43; oraz
- wyjaśniają zakres tego, co może być certyfikowane zgodnie z art. 42 i 43 oraz cel certyfikacji.

RODO umożliwia państwom członkowskim i organom nadzorczym wiele sposobów wdrożenia art. 42 i 43. Wytyczne zawierają porady dotyczące interpretacji i wdrażania przepisów zawartych w art. 42 i 43 oraz pomogą państwom członkowskim, organom nadzorczym i krajowym podmiotom akredytującym w tworzeniu bardziej spójnego, zharmonizowanego podejścia do wdrażania mechanizmów certyfikacji zgodnie z RODO.

Porady zawarte w wytycznych mają znaczenie dla:

- właściwych organów nadzorczych i Europejskiej Rady Ochrony Danych („EROD") przy zatwierdzaniu kryteriów certyfikacji zgodnie z art. 42 ust. 5 i art. 58 ust. 3 lit. f);
- podmiotów certyfikujących podczas opracowywania i przeglądu kryteriów certyfikacji przed przedłożeniem ich do zatwierdzenia właściwemu organowi nadzorczemu zgodnie z art. 42 ust. 5;
- organów nadzorczych przy opracowywaniu własnych kryteriów certyfikacji;
- Komisji Europejskiej, która jest uprawniona do przyjmowania aktów delegowanych w celu określenia wymogów, które należy uwzględnić w przypadku mechanizmów certyfikacji na mocy art. 43 ust. 8;
- EROD przy przekazywaniu Komisji Europejskiej opinii w sprawie wymogów certyfikacyjnych zgodnie z art. 70 ust. 1 lit. q) i art. 43 ust. 8;

ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi."

[5] Patrz Wytyczne Grupy Roboczej Art. 29 w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679 (WP 253).

- krajowych podmiotów akredytujących, które będą musiały wziąć pod uwagę kryteria certyfikacji mając na względzie akredytację podmiotów certyfikujących zgodnie z EN-ISO/IEC 17065/2012 oraz dodatkowe wymogi zgodnie z art. 43; oraz
- administratorów i podmiotów przetwarzających podczas określania własnej strategii przestrzegania RODO i rozważania certyfikacji jako środka wykazania przestrzegania przepisów.

EROD opublikuje oddzielne wytyczne w celu określenia kryteriów zatwierdzania mechanizmów certyfikacji jako narzędzi przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych zgodnie z art. 42 ust. 2.

1.2. Cel certyfikacji na mocy RODO

Art. 42 ust. 1 odnosi się do ustanawiania mechanizmów certyfikacji „mających świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające”.[6]

RODO określa kontekst, w którym zatwierdzone mechanizmy certyfikacji mogą być wykorzystywane jako element do *wykazania przestrzegania* określonych obowiązków administratorów i podmiotów przetwarzających odnośnie:

- wdrożenia i wykazania stosowania odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 24 ust. 1, 3, art. 25 i 32 ust. 1 i 3;

- wystarczających gwarancji (podmiotu przetwarzającego w stosunku do administratora danych), o których mowa w ust. 1 i (podmiot, któremu powierzono przetwarzanie danych, w stosunku do podmiotu przetwarzającego) 4 w art. 28 ust. 5.

Ponieważ certyfikacja sama w sobie nie dowodzi przestrzegania, ale raczej stanowi element, który może być użyty do wykazania zgodności,[7] powinna być przeprowadzana w sposób przejrzysty. Wykazanie przestrzegania wymaga dokumentacji towarzyszącej, w szczególności raportów pisemnych, które nie tylko powtarzają, ale również opisują, w jaki sposób spełnione zostają kryteria i podają powody udzielenia certyfikacji. Obejmuje to ogólny opis poszczególnych decyzji: o udzieleniu, przedłużeniu lub cofnięciu certyfikacji. Powinny także zostać podane powody, argumenty i dowody wynikające z zastosowania kryteriów oraz wnioski, osądy lub konkluzje odnośnie faktów lub przesłanek zebranych podczas certyfikacji.

[6] Art. 42 ust. 2 stanowi ponadto, że można ustanowić mechanizmy certyfikacji w celu wykazania istnienia odpowiednich zabezpieczeń przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych - zostanie to omówione w oddzielnych wytycznych.

[7] Patrz Opinia 3/2010 Grupy Roboczej Art. 29 w sprawie zasady rozliczalności (WP173), punkt 69 podkreśla fakt, że mechanizm certyfikacji „przyczyniłby się do udowodnienia, że administrator danych wypełnił przepis; ponieważ określił i wdrożył odpowiednie środki”. Administrator lub podmiot przetwarzający dane mógł uzyskać certyfikaty dla konkretnej operacji przetwarzania, a jednocześnie naruszyć rozporządzenie.

1.3. Kluczowe pojęcia

W poniższej części omówiono kluczowe pojęcia z art. 42 i 43. Analiza ta pozwala na lepsze zrozumienie podstawowych pojęć i zakresu certyfikacji w ramach RODO.

1.3.1. Interpretacja „certyfikacji"

RODO nie definiuje „certyfikacji". Międzynarodowa Organizacja Normalizacyjna (ISO) przedstawia uniwersalną definicję certyfikacji, która stanowi „dostarczenie 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 zwane „organami oceny zgodności".[8] W EN-ISO/IEC 17000: 2004 - Ocena zgodności - *Słownictwo i zasady ogólne* (których dotyczy norma ISO17065) - certyfikację definiuje się w następujący sposób: „Zaświadczenie przez osobę trzecią ... związane z produktami, procesami i usługami".

Zaświadczenie jest „kwestią oświadczenia, opartego na decyzji podjętej po przeglądzie, że wykazano spełnienie szczególnych wymagań" (rozdział 5.2, ISO 17000: 2004).

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

1.3.2. Mechanizmy certyfikacji, znaki jakości i oznaczenia

RODO nie definiuje „mechanizmów certyfikacji, znaków jakości ani oznaczeń" i stosuje je łącznie. Certyfikat jest oświadczeniem zgodności.[9] Znak jakości lub oznaczenie mogą być użyte jako potwierdzenie pomyślnego zakończenia procedury certyfikacji. Znak jakości lub oznaczenie powszechnie odnosi się do logo lub symbolu, których obecność (oprócz certyfikatu) wskazuje, że przedmiot certyfikacji został niezależnie oceniony i jest zgodny z określonymi wymaganiami określonymi w dokumentach normatywnych, takich jak przepisy, normy lub specyfikacje techniczne.[10] Wymogi te w kontekście certyfikacji na mocy RODO określono w dodatkowych wymaganiach, które uzupełniają zasady akredytacji podmiotów certyfikujących w EN-ISO/IEC 17065/2012 oraz kryteria certyfikacji zatwierdzone przez właściwy organ nadzorczy lub EROD. Certyfikacja na mocy RODO może zostać udzielona wyłącznie po przeprowadzeniu niezależnej oceny dowodów przez akredytowany podmiot certyfikujący lub właściwy organ nadzorczy, stwierdzającej, że kryteria certyfikacji zostały spełnione.

2. Rola organów nadzorczych

Art. 42 ust. 5 stanowi, że certyfikacji udziela akredytowany podmiot certyfikujący lub właściwy organ nadzorczy. RODO nie stanowi, że udzielanie certyfikacji jest obowiązkowym zadaniem organów nadzorczych.[11] Zamiast tego RODO dopuszcza szereg różnych modeli. Na przykład organ nadzorczy może wybrać jedną lub większą liczbę z następujących opcji:

[8] Międzynarodowa Organizacja Normalizacyjna (ISO) patrz https://www.iso.org/conformity-assessment.html
[9] Patrz ISO 17000, do którego odnosi się 17065 .https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-1:v1:en
[10] Patrz podobnie rozporządzenie 765/2008/WE, art. 2 ust. 20 na temat oznaczenia CE oraz ISO 17000:2004, rozdział 3.1 i ISO 17065:2012, rozdział 3.8.
[11] Patrz art. 42 ust. 5 w połączeniu z art. 43 oraz art. 58 ust. 3 lit. f), oraz brak zadania odnoszącego się do tej funkcji w art. 57.

- udzielić certyfikacji samodzielnie w odniesieniu do własnego systemu certyfikacji;
- udzielić certyfikacji samodzielnie w odniesieniu do własnego systemu certyfikacji, ale przekazać całość lub część procesu oceny stronom trzecim;
- stworzyć własny system certyfikacji i powierzyć procedurę certyfikacji podmiotom certyfikującym, które udzielają certyfikacji;
- zachęcać branżę do rozwijania mechanizmów certyfikacji.

Organ nadzorczy będzie musiał również rozważyć swoją rolę w świetle decyzji podjętych na poziomie krajowym dotyczących mechanizmów akredytacji, w szczególności jeżeli sam organ nadzorczy jest uprawniony do akredytowania podmiotów certyfikujących zgodnie z art. 43 ust. 1 RODO. W związku z tym każdy organ nadzorczy określi, jakie podejście zastosować, aby realizować szeroki cel certyfikacji na mocy RODO. Zostanie to określone w kontekście nie tylko zadań i uprawnień w art. 57 i 58, ale również w zakresie uwzględniania certyfikacji jako czynnika, który należy wziąć pod uwagę przy ustalaniu administracyjnych kary pieniężnej, a bardziej ogólnie jako sposób wykazania zgodności.

2.1 Organ nadzorczy jako podmiot certyfikujący

W przypadku gdy organ nadzorczy zdecyduje się na przeprowadzenie certyfikacji, będzie musiał dokładnie ocenić swoją rolę w odniesieniu do przydzielonych mu zadań na mocy RODO. Jego rola powinna być przejrzysta w zakresie wykonywania przydzielonej mu funkcji. Organ taki będzie musiał rozważyć w szczególności podział kompetencji związanych z postępowaniami wyjaśniającymi i egzekwowaniem prawa, aby uniknąć ewentualnych konfliktów interesów.

Działając jako podmiot certyfikujący, organ nadzorczy będzie generalnie musiał zapewnić właściwy mechanizm certyfikacji i opracować własne lub dopasować kryteria certyfikacji. Ponadto każdy organ nadzorczy, który udzielał certyfikacji, ma obowiązek dokonywania okresowego przeglądu tychże (art. 57 ust. 1 lit. o)), oraz jest uprawniony do ich cofnięcia w przypadku, gdy wymogi dotyczące certyfikacji nie są lub przestały być spełniane (art. 58 ust. 2 lit h)). Aby spełnić te wymogi, warto ustanowić procedurę certyfikacji i określić wymagania odnośnie procesu certyfikacji, oraz, jeśli nie określono inaczej np. w prawie krajowym, zawrzeć prawnie wiążącą umowę o świadczenie usług certyfikacyjnych z indywidualną organizacją wnioskującą. Należy dopilnować, aby ta umowa certyfikacyjna wymagała od wnioskodawcy przestrzegania przynajmniej kryteriów certyfikacji, w tym niezbędnych ustaleń w celu przeprowadzenia oceny, monitorowania, oraz przeglądu, w tym dostępu do informacji lub przesłanek, dokumentacji i publikacji sprawozdań i wyników oraz wyjaśniania skarg. Ponadto uzasadnione jest przestrzeganie wymogów i kryteriów określonych w wytycznych dotyczących akredytacji podmiotów certyfikujących oprócz wymogów określonych w art. 43 ust. 2.

2.2 Dalsze zadania organu nadzorczego odnośnie certyfikacji

W państwach członkowskich, w których podmioty certyfikujące są aktywne, na organ nadzorczy, niezależne od jego własnych działań, nałożone są określone uprawnienia i zadania:

- przekazywanie do EROD projektu decyzji, gdy organ planuje zatwierdzenie kryteriów certyfikacji zgodnie z art. 43 ust. 3, 64 ust. 1 lit. c);

- zatwierdzanie kryteriów certyfikacji (art. 58 ust. 3 lit. f)) przed uzyskaniem akredytacji i certyfikacji (art. 42 ust. 5, 43 ust. 2 lit. b)); i
- nakazywanie podmiotowi certyfikującemu (a) odmowy udzielenia certyfikacji, lub (b) cofnięcia certyfikacji w przypadku, gdy wymogi certyfikacji nie są lub przestały być spełniane (art. 58 ust. 2 lit. h).

RODO nakłada na organ nadzorczy zadanie polegające na zatwierdzaniu kryteriów, ale nie opracowywanie kryteriów. W celu zatwierdzenia kryteriów na podstawie art. 42 ust. 5, organ nadzorczy powinien jasno rozumieć, czego należy się spodziewać, w szczególności pod względem zakresu i treści w celu wykazania przestrzegania RODO oraz w odniesieniu do zadań w zakresie monitorowania i egzekwowania stosowania rozporządzenia. EROD zapewni wytyczne w celu zapewnienia zharmonizowanego podejścia przy ocenie kryteriów do celów zatwierdzenia. [12]

Art. 43 ust. 1 wymaga od podmiotów certyfikujących poinformowania organu nadzorczego o zamiarze udzielenia lub przedłużenia certyfikacji, aby umożliwić właściwemu organowi nadzorczemu wykonywanie przysługujących mu uprawnień korygujących zgodnie z art. 58 ust. 2 lit. h). Ponadto art. 43 ust. 5 nakłada również na podmioty certyfikujące obowiązek przedstawienia właściwemu organowi nadzorczemu powodów udzielenia lub cofnięcia żądanej certyfikacji. Mimo że RODO pozwala organom nadzorczym określić sposób otrzymywania, potwierdzania, dokonywania przeglądu i zarządzania tymi informacjami operacyjnie (na przykład może to obejmować rozwiązania technologiczne umożliwiające raportowanie przez podmioty certyfikujące), możliwe jest stworzenie procesu i wprowadzenie kryteriów przetwarzania informacji i raportów odnośnie każdego udanego projektu certyfikacji przeprowadzonego przez podmiot certyfikujący zgodnie z art. 43 ust. 1. Na podstawie tych informacji organ nadzorczy może skorzystać z uprawnienia do nakazania podmiotowi certyfikującemu cofnięcia certyfikacji lub nieudzielenia jej (art. 58 ust. 2 lit. h)) oraz monitorowania i egzekwowania stosowania wymagań i kryteriów certyfikacji na mocy RODO (art. 57 ust. 1 lit. a), art. 58 ust. 2 lit. h)). Pomoże to zharmonizować podejście i porównywalność certyfikacji prowadzonej przez różne podmioty certyfikujące oraz zapewnienie, że informacje na temat statusu certyfikacji organizacji są dostępne organom nadzorczym.

3. Rola podmiotu certyfikującego

Rolą podmiotów certyfikujących jest udzielanie, przeglądanie, przedłużanie i cofanie certyfikacji (art. 42 ust. 5, 7) na podstawie mechanizmu certyfikacji i zatwierdzonych kryteriów (art. 43 ust. 1). Wymaga to od podmiotu certyfikującego lub właściciela systemu certyfikacji[13] określenia i ustanowienia procedur certyfikacji, w tym procedur monitorowania, przeglądania, rozpatrywania skarg i cofania certyfikacji, a także przedstawiania - do celów akredytacji - kryteriów certyfikacji w celu określenia zasad (procedur) zgodnie z którymi udzielana jest certyfikacja, znaki jakości i oznaczenia (art. 43 ust. 2 lit. c)).

Istnienie mechanizmu certyfikacji i kryteriów certyfikacji jest konieczne, aby podmiot certyfikujący uzyskał akredytację na podstawie art. 43. Istotny wpływ na to, co robi podmiot certyfikujący, ma w

[12] W przyszłości w załączniku do tych wytycznych zawarte zostaną odnośne informacje.
[13] Właściciel systemu tworzy kryteria i procedury, ale nie przeprowadza certyfikacji.

szczególności zakres i rodzaj kryteriów certyfikacji, które mają wpływ na procedury certyfikacji i odwrotnie. Konkretne kryteria mogą na przykład wymagać szczególnych metod oceny (np. inspekcje na miejscu, przegląd kodeksu postępowania). Procedury te są obowiązkowe w przypadku akredytacji i zostały dodatkowo wyjaśnione w wytycznych dotyczących akredytacji.[14]

Podmiot certyfikujący jest zobowiązany na mocy RODO do przedstawienia organom nadzorczym informacji, w szczególności na temat indywidualnych certyfikacji, które są niezbędne do monitorowania stosowania mechanizmu certyfikacji (art. 43 ust. 5, art. 58 ust. 2 lit. h)).

4. Zatwierdzanie kryteriów certyfikacji

Kryteria certyfikacji są integralną częścią mechanizmu certyfikacji. Co za tym idzie RODO wymaga zatwierdzenia kryteriów certyfikacji przez właściwy organ nadzorczy (art. 42 ust. 5 i 43 ust. 2 lit. b)).

EROD identyfikuje następujące cele zatwierdzania kryteriów certyfikacji:

- właściwe odzwierciedlenie wymogów i zasad dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych określonych w rozporządzeniu (UE) 2016/679; oraz
- przyczynianie się do spójnego stosowania RODO.

Zatwierdzenie jest przyznawane na podstawie tego, że wymóg zawarty w RODO, zgodnie z którym mechanizm certyfikacji ma umożliwiać administratorom i podmiotom przetwarzającym wykazanie przestrzegania RODO, znajduje pełne odzwierciedlenie w kryteriach certyfikacji.

4.1. Termin zatwierdzenia

Kryteria certyfikacji muszą być zatwierdzone przez właściwy organ nadzorczy przed rozpoczęciem procesu akredytacji lub w jego trakcie. Zatwierdzenie jest również wymagane w przypadku zaktualizowanych i dalszych systemów lub zbiorów kryteriów zgodnie z ISO 17065 przed ich zastosowaniem w mechanizmach certyfikacji (art. 42 ust. 5, art. 43 ust. 2 lit. b)).

4.2. Właściwy organ nadzorczy

Podmiot certyfikujący może udzielić certyfikacji tylko w danym państwie członkowskim zgodnie z kryteriami zatwierdzonymi przez organ nadzorczy w tym państwie członkowskim. Innymi słowy, kryteria certyfikacji muszą zostać zatwierdzone przez właściwy organ nadzorczy, gdy podmiot certyfikujący zamierza oferować certyfikację i uzyskuje akredytację. Alternatywnie podmiot certyfikujący może również udzielić certyfikacji zgodnie z kryteriami zatwierdzonymi przez EROD, co może skutkować przyznaniem europejskiego znaku jakości ochrony danych.

4.3. Europejski znak jakości ochrony danych

Kryteria certyfikacji zatwierdzone przez EROD zgodnie z art. 63 mogą prowadzić do ustanowienia europejskiego znaku jakości ochrony danych (art. 42 ust. 5). W świetle obowiązujących konwencji

[14] Patrz projekt Wytycznych Grupy Roboczej Art. 29 dotyczących akredytacji przyjętych 6 lutego 2018 r. (WP 261).

dotyczących certyfikacji i akredytacji, EROD przyznaje, że pożądane jest uniknięcie rozdrobnienia rynku certyfikacji jakości ochrony danych. EROD odnotowuje, że art. 42 ust. 1 stanowi, że państwa członkowskie, organy nadzorcze, Rada i Komisja zachęcają do ustanowienia mechanizmów certyfikacji, *w szczególności na poziomie Unii*.

Wniosek o zatwierdzenie do EROD powinien określać zamiar wnioskującego podmiotu certyfikującego proponowania kryteriów w mechanizmie certyfikacji skierowanym do administratorów i podmiotów przetwarzających w kilku państwach członkowskich.

W oparciu o art. 42 ust. 5 mechanizm europejskiego znaku jakości ochrony danych, jak również jego kryteria, muszą uwzględniać, w stosownych przypadkach, krajowe przepisy sektorowe, np. odnośnie przetwarzania danych w szkołach publicznych[15] i przewidywać zastosowanie w całej Europie.

Wymogi dotyczące europejskiego znaku jakości ochrony danych obejmują:

- kryteria zatwierdzone przez Radę:
  - stosowanie we wszystkich jurysdykcjach, odzwierciedlające, w stosownych przypadkach, krajowe wymogi prawne i przepisy sektorowe;
- opis mechanizmu certyfikacji określający:
  - umowy certyfikacyjne, uznające ogólnoeuropejskie wymagania;
  - język sprawozdań skierowanych do wszystkich zainteresowanych organów nadzorczych.

Jeżeli kryteria certyfikacji zostały zatwierdzone przez Radę zgodnie z art. 42 ust. 5, akredytowane podmioty certyfikujące mogą przeprowadzać certyfikację zgodnie z tymi kryteriami na poziomie Unii. Kryteria w ramach tego ogólnoeuropejskiego mechanizmu certyfikacji mogą obejmować operacje przetwarzania danych prowadzone w państwach członkowskich.

5. Opracowanie kryteriów certyfikacji

RODO ustanawiło ramy dla rozwoju kryteriów certyfikacji. O ile podstawowe wymagania dotyczące procedury certyfikacji zostały omówione w art. 42 i 43, a jednocześnie zapewniają podstawowe kryteria procedur certyfikacji, podstawa kryteriów certyfikacji musi wynikać z zasad i reguł RODO i pomóc w zapewnieniu ich przestrzegania.

Opracowanie kryteriów certyfikacji powinno uwzględniać nie tylko popyt na rynku, ale także w celu ich pomyślnego zatwierdzenia, należy również wziąć pod uwagę weryfikowalność, istotność i odpowiedniość kryteriów certyfikacji w celu wykazania przestrzegania rozporządzenia. Kryteria certyfikacji powinny być sformułowane w taki sposób, aby były jasne i zrozumiałe oraz aby pozwalały na praktyczne zastosowanie.

[15] RODO przewiduje klauzule otwarte. Państwa członkowskie mogą utrzymać lub wprowadzić bardziej szczegółowe przepisy w celu dostosowania stosowania zasad RODO w odniesieniu do przetwarzania pod kątem zgodności z określonymi wymogami lub szczególnymi sytuacjami przetwarzania.

Podczas opracowywania kryteriów certyfikacji w stosownych przypadkach uwzględnia się między innymi następujące aspekty zgodności wspierające ocenę operacji przetwarzania w stosownych przypadkach:

- zgodność przetwarzania z prawem zgodnie z art. 6;
- zasady przetwarzania danych zgodnie z art. 5;
- prawa osób, których dane dotyczą, zgodnie z art. 12-23;
- obowiązek zgłaszania naruszeń ochrony danych zgodnie z art. 33;
- obowiązek ochrony danych w fazie projektowania oraz domyślnej ochrony danych, zgodnie z art. 25;
- to, czy przeprowadzono ocenę skutków dla ochrony danych, zgodnie z art. 35 ust. 7 lit. d), jeśli dotyczy; i
- środki techniczne i organizacyjne ustanowione zgodnie z art. 32.

Zakres, w jakim te uwarunkowania znajdują odzwierciedlenie w kryteriach, może się różnić w zależności od zakresu certyfikacji, który może obejmować rodzaj operacji przetwarzania i obszar (np. sektor zdrowia) certyfikacji.

5.1. Co może być objęte certyfikacją na mocy RODO?

EROD jest zdania, że RODO określa szeroki zakres tego, co może być objęte certyfikacją na mocy RODO, o ile sednem jest pomoc w wykazaniu przestrzegania przedmiotowego rozporządzenia podczas operacji przetwarzania danych przez administratorów i podmioty przetwarzające (art. 42 ust. 1).

Oceniając operację przetwarzania, należy w stosownych przypadkach wziąć pod uwagę następujące trzy podstawowe elementy:

1. dane osobowe (zakres przedmiotowy RODO);
2. systemy techniczne - infrastrukturę taką jak sprzęt i oprogramowanie wykorzystywane do przetwarzania danych osobowych; i
3. procesy i procedury związane z operacją(ami) przetwarzania.

Każdy element wykorzystywany w operacjach przetwarzania musi podlegać ocenie zgodnie z ustalonymi kryteriami. Wpływ mogą mieć co najmniej cztery różne istotne czynniki: 1) organizacja i struktura prawna administratora lub podmiotu przetwarzającego; 2) dział, środowisko i osoby zaangażowane w proces(y) przetwarzania; 3) opis techniczny elementów podlegających ocenie, i wreszcie 4) infrastruktura informatyczna wspierająca operację przetwarzania, w tym systemy operacyjne, systemy wirtualne, bazy danych, systemy uwierzytelnienia i autoryzacji, routery i zapory typu firewall, systemy pamięci masowej, infrastruktura komunikacyjna lub dostęp do Internetu oraz powiązane środki techniczne.[16]

Wszystkie trzy podstawowe elementy są istotne dla tworzenia procedur i kryteriów certyfikacji. W zależności od przedmiotu certyfikacji zakres, w jakim są one brane pod uwagę, może być różny.

[16] Należy pamiętać, że operacje przetwarzania nie są tożsame z wykorzystaniem określonego rodzaju technologii lub programu.

Przykładowo w niektórych przypadkach niektóre elementy mogą zostać pominięte, jeśli zostaną uznane za nieistotne dla przedmiotu certyfikacji.

W celu dokładniejszego określenia, co może być objęte certyfikacją na mocy RODO, rozporządzenie to zawiera dodatkowe wytyczne. Z art. 42 ust. 7 wynika, że certyfikacja na mocy RODO udzielana jest tylko administratorom danych i podmiotom przetwarzającym dane, co wyklucza na przykład certyfikację osób fizycznych, takich jak inspektorów ochrony danych. Art. 43 ust. 1 lit. b) odnosi się do normy ISO 17065, która przewiduje akredytację podmiotów certyfikujących oceniających zgodność produktów, usług i procesów.[17] Operacja przetwarzania lub zestaw operacji może prowadzić do powstania produktu lub usługi w terminologii ISO 17065, które jako takie mogą być przedmiotem certyfikacji. Przykładowo przetwarzanie danych osobowych pracowników w celu wypłaty wynagrodzenia lub zarządzania urlopami jest zbiorem operacji w rozumieniu RODO i może skutkować produktem, procesem lub usługą w terminologii ISO.

Na podstawie tych rozważań EROD jest zdania, że zakres certyfikacji na mocy RODO jest ukierunkowany na operacje przetwarzania lub zestawy operacji. Mogą one obejmować procesy zarządzania w sensie środków organizacyjnych, a zatem jako integralne części operacji przetwarzania (np. proces zarządzania ustanowiony w celu rozpatrywania skarg w ramach przetwarzania danych osobowych pracowników w celu wypłaty wynagrodzenia).

Aby ocenić zgodność operacji przetwarzania z kryteriami certyfikacji, należy podać konkretny przypadek. Na przykład zgodność wykorzystania infrastruktury technicznej wdrożonej w operacji przetwarzania zależy od kategorii danych, które mają być przetwarzane. Środki organizacyjne zależą od kategorii i ilości danych oraz infrastruktury technicznej wykorzystywanej do przetwarzania, z uwzględnieniem charakteru, zakresu, treści i celów przetwarzania, a także ryzyka naruszenia praw lub wolności osób, których sprawa dotyczy.

Co więcej należy pamiętać, że aplikacje informatyczne mogą się znacznie różnić, nawet jeśli służą one takim samym celom przetwarzania. Dlatego należy to uwzględnić przy określaniu zakresu mechanizmów certyfikacji i opracowywaniu kryteriów certyfikacji, tj. zakres certyfikacji i kryteria nie powinny być na tyle wąskie, aby wykluczyć aplikacje informatyczne zaprojektowane inaczej.

5.2. Określanie przedmiotu certyfikacji

Zakres mechanizmu certyfikacji należy odróżnić od przedmiotu - zwany także celem ewaluacji (ToE) - w poszczególnych projektach certyfikacyjnych w ramach mechanizmu certyfikacji.[18] Mechanizm certyfikacji może określać jego zakres albo ogólnie, albo w odniesieniu do określonego typu lub obszaru operacji przetwarzania i może już identyfikować przedmioty certyfikacji, które wchodzą w zakres mechanizmu certyfikacji (np. bezpieczne przechowywanie i ochrona danych osobowych zawartych w skarbcu cyfrowym). W każdym przypadku wiarygodna, racjonalna ocena zgodności może mieć miejsce tylko wtedy, gdy szczegółowo opisany zostanie pojedynczy przedmiot projektu

[17] Patrz EN-ISO/IEC 17065/2012 Ocena zgodności - Wymagania dla podmiotów certyfikujących produkty, procesy i usługi.
[18] Patrz także Wspólne kryteria oceny bezpieczeństwa technologii informatycznych, Część 1: Wprowadzenie i model ogólny, kwiecień 2017, wersja 3.1, przegląd 5.

certyfikacji[19]. Należy jasno określić, które operacje przetwarzania są objęte certyfikacją, a następnie które główne komponenty, t.j. dane, procesy i infrastruktura techniczna, będą oceniane, a które nie. Należy przy tym zawsze uwzględnić i opisać interfejsy do innych procesów. Rzecz jasna to, co nie jest znane, nie może stanowić części oceny, a zatem nie może być certyfikowane. W każdym przypadku indywidualny przedmiot certyfikacji musi mieć znaczenie w zakresie certyfikacji i nie powinien wprowadzać w błąd użytkownika ani konsumenta.

[Przykład 1]

Bank oferuje swoim klientom stronę internetową dla celów bankowości internetowej. W ramach tej usługi istnieje możliwość dokonywania przelewów, nabywania udziałów, tworzenia zleceń stałych i zarządzania kontem. Bank chce uzyskać certyfikację poniższych elementów w ramach mechanizmu certyfikacji ochrony danych w ogólnym zakresie w oparciu o ogólne kryteria:

a) Bezpieczne logowanie
   Bezpieczne logowanie jest operacją przetwarzania, która jest zrozumiała dla użytkownika końcowego i która jest istotna z punktu widzenia ochrony danych, ponieważ odgrywa ważną rolę w zapewnianiu bezpieczeństwa danych osobowych. Dlatego ta operacja przetwarzania jest niezbędna do bezpiecznego logowania, a zatem może stanowić znaczący ToE, jeśli certyfikat wyraźnie stwierdza, że tylko operacja przetwarzania logowania jest certyfikowana.

b) Front-end sieciowy
   Podczas gdy front-end sieciowy może być istotny z punktu widzenia ochrony danych, nie jest zrozumiały dla użytkownika końcowego i dlatego nie może być znaczącym ToE. Ponadto nie jest jasne dla użytkownika, które usługi na stronie internetowej, a tym samym operacje przetwarzania, są objęte certyfikacją.

c) Bankowość internetowa
   Front-end i back-end sieciowy to operacje przetwarzania prowadzone w ramach usługi bankowości internetowej, które mogą mieć znaczenie dla użytkownika. W tym kontekście muszą one być uwzględnione w ToE. Operacje przetwarzania niezwiązane bezpośrednio ze świadczeniem usług bankowości internetowej, takie jak operacje przetwarzania w celu zapobiegania praniu pieniędzy, mogą być wyłączone z ToE.

Jednakże usługi bankowości internetowej oferowane przez bank za pośrednictwem strony internetowej mogą również obejmować inne usługi, które z kolei wymagają własnych operacji przetwarzania. W tym kontekście inne usługi mogą obejmować na przykład ofertę produktu ubezpieczeniowego. Ponieważ ta dodatkowa usługa nie jest bezpośrednio związana z celem świadczenia usług bankowości internetowej, może być wyłączona z ToE. Jeśli ta dodatkowa usługa (ubezpieczenie) zostanie wykluczona z ToE, interfejsy dla tej usługi zintegrowane na stronie internetowej są częścią ToE i dlatego muszą zostać opisane, aby wyraźnie odróżnić usługi. Taki opis jest niezbędny do określenia i ewaluacji ewentualnych przepływów danych między obiema usługami.

[Przykład 2]

Bank oferuje swoim klientom usługę umożliwiającą łączenie informacji związanych z różnymi rachunkami i kartami kredytowymi z kilku banków (agregacja konta). Bank chce, aby jego usługa została objęta certyfikacją na mocy RODO. Właściwy organ nadzorczy zatwierdził specjalny zbiór kryteriów

[19] Nazywany także celem ewaluacji, ang. target of evaluation, ToE, por. np. Wspólne Kryteria.

certyfikacji koncentrujących się na tego rodzaju działalności. Zakres mechanizmu certyfikacji obejmuje tylko następujące aspekty zgodności:

- uwierzytelnianie użytkownika; oraz
- akceptowalne sposoby uzyskiwania danych, które mają być zbierane z innych banków/serwisów.

Ponieważ zakres tego mechanizmu certyfikacji definiuje sam w sobie ToE, nie można sensownie zawęzić ToE w proponowanym zakresie.

5.3. Metody ewaluacji i metodologia oceny

Ocena zgodności w celu wykazania przestrzegania wymogów RODO w operacji przetwarzania wymaga zdefiniowania i określenia metod ewaluacji i metodologii oceny. Istotne jest, czy informacje do oceny są zbierane wyłącznie z dokumentacji, czy też są gromadzone aktywnie na miejscu i przez dostęp bezpośredni lub pośredni. Sposób gromadzenia informacji ma wpływ na znaczenie certyfikacji i dlatego powinien zostać określony i opisany.

Procedury udzielania i okresowego przeglądu certyfikacji powinny zawierać specyfikacje pozwalające określić odpowiedni poziom ewaluacji (dogłębność i szczegółowość) w celu spełnienia kryteriów certyfikacji i powinny obejmować:

- informacje na temat i specyfikację zastosowanych metod badań i wniosków zebranych podczas audytów na miejscu lub z dokumentacji,
- metody ewaluacji koncentrujące się na operacjach przetwarzania (danych, systemach, procesach) i celu przetwarzania,
- identyfikację kategorii danych, potrzeb w zakresie ochrony oraz określenie, czy zaangażowani są administratorzy lub osoby trzecie,
- określenie ról i istnienia mechanizmu kontroli dostępu zdefiniowanego wokół ról i obowiązków.

Poziom oceny ma wpływ na znaczenie certyfikacji. Poprzez zmniejszenie poziomu ewaluacji w celu zmniejszenia kosztów lub w celach pragmatycznych znaczenie certyfikacji ochrony danych zostanie zmniejszone. Z drugiej strony jeżeli chodzi o decyzje dotyczące szczegółowości oceny, certyfikacja może przewyższać możliwości finansowe wnioskodawcy, a często także zdolność podmiotów ewaluujących i audytujących. W celu wykazania zgodności nie zawsze konieczne jest przeprowadzenie bardzo szczegółowej analizy wykorzystywanych systemów informatycznych.

5.4. Dokumentacja oceny

Dokumentacja odnośnie certyfikacji powinna być kompletna i wyczerpująca, ponieważ brak dokumentacji oznacza, że nie można przeprowadzić właściwej oceny. Podstawową funkcją dokumentacji certyfikacyjnej jest zapewnienie przejrzystości w procesie oceny w ramach mechanizmu certyfikacji. Dokumentacja zawiera odpowiedzi na pytania dotyczące wymagań określonych prawem. Następnie ocena umożliwia porównanie dokumentacji certyfikacyjnej z faktycznym stanem na miejscu i kryteriami certyfikacji.

Kompleksowa dokumentacja tego, co zostało certyfikowane i zastosowanej metodologii służy zapewnieniu przejrzystości. Zgodnie z art. 43 ust. 2 lit. c) mechanizmy certyfikacji powinny ustanawiać procedury umożliwiające przegląd udzielonej certyfikacji. Aby umożliwić organowi nadzorczemu ocenę, czy i w jakim zakresie można uznać certyfikację podczas formalnych postępowań wyjaśniających, najodpowiedniejszym środkiem komunikacji może być szczegółowa dokumentacja. Dokumentacja opracowana podczas oceny powinna zatem skupiać się na trzech głównych aspektach:

- spójności realizowanych metod oceny;
- metodach oceny ukierunkowanych na wykazanie zgodności przedmiotu certyfikacji z kryteriami certyfikacji, a tym samym z rozporządzeniem; i
- tym, że wyniki oceny zostały potwierdzone przez niezależny i bezstronny podmiot certyfikujący.

5.5. Dokumentacja wyników

Motyw 100 zawiera informacje na temat celów wprowadzenia 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."*

Ważną rolę w celu zwiększenia przejrzystości odgrywa dokumentowanie i przekazywanie wyników. Mechanizmy certyfikacji ukierunkowane na osoby, których dane dotyczą, powinny zapewniać łatwo dostępne, zrozumiałe i istotne informacje na temat certyfikowanych operacji przetwarzania. Informacje te powinny przynajmniej obejmować:

- opis celu ewaluacji (ToE);
- kryteria zastosowane do konkretnego ToE;[20]
- metodologię oceny kryteriów (ocena na miejscu, dokumentacja itp.); oraz
- okres ważności certyfikatu.

6. Wytyczne dotyczące określania kryteriów certyfikacji

Kryteria certyfikacji są integralną częścią mechanizmu certyfikacji. Procedura certyfikacji obejmuje wymagania dotyczące tego, w jaki sposób, przez kogo, w jakim zakresie i w jakim stopniu szczegółowości dokonywana będzie ocena w poszczególnych projektach certyfikacyjnych odnośnie konkretnego przedmiotu lub celu oceny (ToE). Kryteria certyfikacji określają nominalne wymagania, względem których ocenia się faktyczną operację przetwarzania zdefiniowaną w ToE. Wytyczne dotyczące określania kryteriów certyfikacji zapewnią ogólne rady, które ułatwią ocenę kryteriów certyfikacji do celów zatwierdzenia.

Podczas zatwierdzania lub określania kryteriów certyfikacji należy wziąć pod uwagę następujące ogólne kwestie. Kryteria certyfikacji powinny:

- być jednolite i weryfikowalne,

[20] Patrz rozdział 5.

- podlegać audytowi w celu ułatwienia oceny operacji przetwarzania danych na mocy RODO, określając w szczególności cele i wskazówki wykonawcze dla osiągnięcia tych celów;
- być istotne w odniesieniu do docelowej grupy odbiorców (np. B2B i przedsiębiorstwa - konsument (B2C));
- uwzględniać i, w stosownych przypadkach, współgrać z innymi normami (takimi jak normy ISO, normy na poziomie krajowym); i
- być elastyczne i skalowalne w celu zastosowania do różnych typów i rozmiarów organizacji, w tym mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw zgodnie z art. 42 ust. 1 oraz podejścia opartego na ryzyku zgodnie z motywem 77.

Mała lokalna firma, na przykład sprzedawca detaliczny, przeprowadza mniej złożone operacje przetwarzania. O ile wymogi dotyczące legalności operacji przetwarzania są takie same, należy wziąć pod uwagę zakres przetwarzania danych i jego złożoność. Wynika stąd, że potrzebne są mechanizmy certyfikacji i kryteria, które są skalowalne zgodnie z daną działalnością przetwarzania.

6.1. Istniejące standardy

Podmioty certyfikujące będą musiały rozważyć, w jaki sposób konkretne kryteria uwzględniają istniejące odpowiednie normy techniczne lub krajowe inicjatywy prawne i regulacyjne. Idealnym rozwiązaniem jest interoperacyjność kryteriów i istniejących standardów, które mogą pomóc administratorowi lub podmiotowi przetwarzającemu w wypełnieniu zobowiązań wynikających z RODO. Jednak podczas gdy standardy branżowe często koncentrują się na ochronie i bezpieczeństwie organizacji przed zagrożeniami, RODO jest ukierunkowane na ochronę praw podstawowych osób fizycznych. Ta odmienna perspektywa musi być brana pod uwagę przy projektowaniu kryteriów lub zatwierdzaniu kryteriów lub mechanizmów certyfikacji opartych na standardach branżowych.

6.2. Określanie kryteriów

Kryteria certyfikacji muszą być zgodne z deklaracją (oświadczeniem lub stwierdzeniem) mechanizmu lub schematu certyfikacji i spełniać oczekiwania, które wywołuje. Nazwa określa również zakres zastosowania, a w konsekwencji określenie kryteriów.

[Przykład 3]

Mechanizm o nazwie "HealthPrivacyMark" („Znak jakości – prywatność w służbie zdrowia”) powinien ograniczyć swój zakres do sektora służby zdrowia. Nazwa znaku jakości wzbudza oczekiwanie, że zbadane zostały wymogi ochrony danych w związku z danymi dotyczącymi zdrowia. W związku z tym kryteria tego mechanizmu muszą być odpowiednie do oceny wymagań w zakresie ochrony danych w tym sektorze.

[Przykład 4]

Mechanizm, który odnosi się do certyfikacji operacji przetwarzania obejmujących systemy zarządzania w przetwarzaniu danych, powinien określać kryteria, które pozwalają na uznawanie i ocenę procesów zarządzania oraz wspierających środków technicznych i organizacyjnych.

[Przykład 5]

Kryteria dotyczące mechanizmu związanego z chmurą obliczeniową muszą uwzględniać specjalne

wymagania techniczne niezbędne do korzystania z usług w chmurze. Przykładowo jeżeli serwery są używane poza UE, kryteria muszą uwzględniać warunki określone w rozdziale V RODO w odniesieniu do przekazywania danych do państw trzecich.

Kryteria zaprojektowane tak, aby pasowały do różnych ToE w różnych sektorach i/lub państwach członkowskich powinny: zezwalać na realizowanie różnych scenariuszy; pozwalać na określenie odpowiednich środków w celu dopasowania do małych, średnich lub dużych operacji przetwarzania i odzwierciedlać ryzyko związane ze zmiennym prawdopodobieństwem i wagą dla praw i wolności osób fizycznych zgodnie z RODO. W związku z tym procedury certyfikacji (np. dotyczące dokumentacji, testowania lub dogłębności oceny), które uzupełniają kryteria, muszą odpowiadać na te potrzeby oraz umożliwiać i wprowadzać reguły, na przykład w celu zastosowania odpowiednich kryteriów w poszczególnych projektach certyfikacyjnych. Kryteria w tym zakresie muszą ułatwiać ocenę, czy zapewniono wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych.

6.3. Okres ważności kryteriów certyfikacji

Mimo że kryteria certyfikacji muszą pozostawać wiarygodne w miarę upływu czasu, nie powinny być „wyryte w kamieniu”. Podlegają one rewizji, na przykład gdy:

- ramy prawne zostały zmienione;
- warunki i przepisy są interpretowane wyrokami Europejskiego Trybunału Sprawiedliwości; lub
- ewoluuje stan rozwoju techniki.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

Załącznik: Zadania i prawa organów nadzorczych odnośnie certyfikacji zgodnie z RODO

	Przepisy	**Wymogi**
Zadania	Art. 43 ust. 6	Wymaga od organu nadzorczego upublicznienia kryteriów, o których mowa w art. 42 ust. 5, w łatwo dostępny sposób oraz przekazania ich Radzie.
	Art. 57 ust. 1 lit. n)	Wymaga od organu nadzorczego zatwierdzenia kryteriów certyfikacji zgodnie z art. 42 ust. 5.
	Art. 57 ust. 1 lit. o)	Stanowi, że w stosownych przypadkach (tj. w przypadku wydania certyfikatu) dokonuje okresowego przeglądu certyfikacji zgodnie z art. 42 ust. 7.
	Art. 64 ust. 1 lit. c)	Wymaga od organu nadzorczego przekazania projektu decyzji Radzie, jeśli ma on na celu zatwierdzenie kryteriów certyfikacji, o których mowa w art. 42 ust. 5.
Prawa	Art. 58 ust. 1 lit. c)	Zapewnia, że organ nadzorczy jest uprawniony do dokonywania przeglądów certyfikacji zgodnie z art. 42 ust. 7;
	Art. 58 ust. 2 lit. h)	Zapewnia organowi nadzorczemu prawo do cofnięcia lub nakazania podmiotowi certyfikującemu cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu nieudzielenia certyfikacji.
	Art. 58 ust. 3 li.t e)	Stanowi, że organ nadzorczy ma prawo do akredytowania podmiotów certyfikujących.
	Art. 58 ust. 3 lit. f)	Stanowi, że organ nadzorczy ma prawo do udzielania certyfikacji i zatwierdzania kryteriów certyfikacji.