Dodatkowe wymogi akredytacji podmiotów certyfikujących

8 grudnia 2023 r.

Wersja 1.2

URZĄD OCHRONY DANYCH OSOBOWYCH

Wersja 1.0	31 stycznia 2022 r.	Projekt dodatkowych wymogów akredytacji podmiotów certyfikujących na potrzeby opinii EROD.
Wersja 1.1	31 stycznia 2023 r.	Projekt dodatkowych wymogów akredytacji podmiotów certyfikujących po uwzględnieniu Opinii 11/2022 w sprawie projektu decyzji właściwego organu nadzorczego w Polsce w sprawie zatwierdzenia wymogów akredytacji podmiotów certyfikujących zgodnie z art. 43 ust. 3 (RODO), przyjętej przez Europejską Radę Ochrony Danych w dniu 4 lipca 2022 r.
Wersja 1.2	8 grudnia 2023 r.	Dodatkowe wymogi akredytacji podmiotów certyfikujących zatwierdzone przez Prezesa UODO po uwzględnieniu Opinii 11/2022 EROD i aktualizacji publikatorów aktów prawnych w nich przywołanych.

Wstęp

Zgodnie z motywem 100 i art. 42 ust. 1 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1, z późn. zm.), zwane dalej RODO, Prezes Urzędu Ochrony Danych Osobowych (dalej: Prezes Urzędu) zachęca do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z RODO. Te mechanizmy certyfikacji oraz znaki jakości i oznaczenia mają na celu nie tylko umożliwienie osobom, których dane osobowe będą przetwarzane, szybko ocenić stopień ich ochrony, ale i pozwolą podmiotom zobowiązanym na wdrożenie odpowiednich środków technicznych i organizacyjnych w rozumieniu ogólnego rozporządzenia o ochronie danych, w tym w szczególności administratorom i podmiotom przetwarzającym, wykazać zgodność z RODO.

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

W Polsce, zgodnie z art. 12 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781) w związku z art. 43 ust. 1 lit. b) RODO **Polskie Centrum Akredytacji (PCA)** jest uprawnione do udzielania akredytacji podmiotów certyfikujących.

PCA jest krajową jednostką akredytującą upoważnioną do akredytacji jednostek oceniających zgodność na podstawie ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. z 2022 r. poz. 1854). Podmiot ten posiada status państwowej osoby prawnej i jest nadzorowany przez ministra właściwego do spraw gospodarki.

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającym wymagania w zakresie akredytacji i uchylającym rozporządzenie (EWG) nr 339/93 (Dz.U. UE. L.

2008.218.30 z późn. zm.), PCA zostało wskazane jako jedyna krajowa jednostka akredytująca w świetle ww. rozporządzenia.

W związku z powyższym Polskie Centrum Akredytacji będzie udzielało akredytacji podmiotów certyfikujących na podstawie:

- normy ISO/IEC 17065/2012 oraz
- „Dodatkowych wymogów akredytacji podmiotów certyfikujących" w rozumieniu art. 43 ust. 3 RODO, określonych przez Prezesa Urzędu w oparciu o procedurę określoną w RODO.

Treść „Dodatkowych wymogów akredytacji podmiotów certyfikujących" została określona w niniejszym dokumencie.

Akredytacja podmiotów certyfikujących udzielana będzie na maksymalny okres pięciu lat.

Podmiot ubiegający się o akredytację w rozumieniu art. 43 RODO zobowiązany jest skontaktować się z Polskim Centrum Akredytacji.

Warunki współpracy między Prezesem Urzędu Ochrony Danych Osobowych a Polskim Centrum Akredytacji jako krajową jednostką akredytującą w rozumieniu art. 43 ust. 1 lit. b RODO mogą zostać określone w porozumieniu o współpracy, o którym mowa w art. 14 ust. 5 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. W dokumencie tym można określić role i obowiązki związane z monitorowaniem działalności podmiotów certyfikujących i wzajemnym przekazywaniem informacji dotyczących tych podmiotów. Po zawarciu dokument ten będzie dostępny zarówno na stronie internetowej Urzędu Ochrony Danych Osobowych, jak i na stronie internetowej Polskiego Centrum Akredytacji.

Polskie Centrum Akredytacji oraz podmioty certyfikujące są zobowiązane do wskazania Prezesowi Urzędu adresu elektronicznej skrzynki podawczej w rozumieniu art. 3 pkt 17 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57) i wykorzystywania jej w komunikacji z Prezesem Urzędu związanej z akredytacją podmiotów certyfikujących i certyfikacją.

§ 1.

Zakres

Niniejszy dokument określa dodatkowe wymogi w stosunku do normy ISO/IEC 17065/2012 dotyczące oceny kompetencji, spójnego funkcjonowania i bezstronności podmiotów certyfikujących w rozumieniu art. 42 ust. 5 RODO.

Zakres normy ISO/IEC 17065/2012 stosuje się zgodnie z RODO. Dalsze informacje znajdują się w wytycznych Europejskiej Rady Ochrony Danych (EROD) w sprawie akredytacji[1] i certyfikacji[2].

Szeroki zakres normy ISO/IEC 17065/2012, obejmujący produkty, procesy i usługi, nie powinien prowadzić do zaniżania, ani zastępowania wymogów RODO. Na przykład mechanizm zarządzania nie może być jedynym elementem mechanizmu certyfikacji, ponieważ certyfikacja zgodnie z art. 42 ust. 1 RODO musi obejmować operacje przetwarzania danych osobowych.

Zgodnie z art. 15 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych certyfikacji udziela podmiot certyfikujący na wniosek:

- administratora,
- podmiotu przetwarzającego,
- producenta,
- albo podmiotu wprowadzającego usługę lub produkt na rynek.

Producenci, albo podmioty wprowadzające usługę lub produkt na rynek muszą posiadać status administratora lub podmiotu przetwarzającego w procesie przetwarzania danych osobowych, w którym ww. usługa lub produkt będą stosowane. Zgodnie z art. 15 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych nadrzędne są zasady ujęte w art. 42 RODO, precyzujące zasady certyfikacji procesów przetwarzania danych osobowych.

Mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych wydawane produktom i usługom obejmującym operacje

[1] Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_pl

[2] Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_pl

przetwarzania danych osobowych umożliwią szybką ocenę ich poziomu ochrony danych.

Zakres mechanizmu certyfikacji (np. certyfikacja operacji przetwarzania w chmurze) jest uwzględniany w ocenie przeprowadzanej przez jednostkę akredytującą w trakcie procesu akredytacji, w szczególności w odniesieniu do kryteriów, wiedzy fachowej i metodyki oceny.

§ 2.

Odniesienia normatywne

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

§ 3.

Terminy i definicje

Terminy i definicje zawarte w wytycznych dotyczących akredytacji i certyfikacji mają zastosowanie i mają pierwszeństwo przed definicjami ISO. Poniżej przedstawiono główne definicje użyte w niniejszym dokumencie:

1. **RODO** – rozporządzenie 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 (Dz. Urz. UE L 119 z 4.5.2016, str. 1, z późn. zm.);

2. **u.o.d.o**. – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781);

3. **Rada** – Europejska Rada Ochrony Danych;

4. **Wytyczne Rady dotyczące akredytacji** – Wytyczne nr 4/2018 w sprawie akredytacji podmiotów certyfikujących na mocy art. 43 RODO (2016/679);

5. **Wytyczne Rady dotyczące certyfikacji** – Wytyczne 1/2018 w sprawie certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 RODO;

6. **Organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych;

7. **PCA - Polskie Centrum Akredytacji** – krajowa jednostka akredytująca, wyłączna jednostka w państwie członkowskim wskazana zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008, która dokonuje akredytacji na podstawie upoważnienia udzielonego przez państwo;

8. **Certyfikacja** – ocena i bezstronne poświadczenie przez stronę trzecią, że wykazano spełnienie kryteriów certyfikacji w odniesieniu do operacji przetwarzania prowadzonych przez administratora lub podmiot przetwarzający;

9. **Akredytacja** – poświadczenie przez Polskie Centrum Akredytacji, że podmiot certyfikujący posiada kwalifikacje do przeprowadzania certyfikacji zgodnie z art. 42 i 43 RODO, z uwzględnieniem normy ISO/IEC 17065/2012 oraz niniejszych dodatkowych wymogów ustanowionych przez organ nadzorczy lub EROD. Więcej informacji na temat interpretacji akredytacji do celów art. 43 RODO można znaleźć w sekcji 3 Wytycznych Rady dotyczących akredytacji;

10. **Podmiot certyfikujący** – podmiot prowadzący system certyfikacji, w tym oceniający zgodność przedmiotu oceny;

11. **Kryteria certyfikacji** – kryteria, na podstawie których dokonuje się oceny operacji przetwarzania prowadzonych przez Wnioskodawcę lub Klienta w odniesieniu do danego systemu certyfikacji;

12. **System certyfikacji** – system odnoszący się do określonych wyrobów, procesów i usług, do których mają zastosowanie te same wymogi, szczegółowe zasady i procedury. Obejmuje on kryteria certyfikacji i metodykę oceny;

13. **Mechanizm certyfikacji** – zatwierdzony system certyfikacji, który jest dostępny dla Wnioskodawcy. Jest to usługa świadczona przez akredytowany podmiot certyfikujący w oparciu o zatwierdzone kryteria i metodykę oceny. Jest to system, za pomocą którego Wnioskodawca uzyskuje certyfikację;

14. **Przedmiot oceny** – przedmiot certyfikacji. W przypadku certyfikacji RODO będą to odpowiednie operacje przetwarzania, o których ocenę i certyfikację wnosi Wnioskodawca;

15. **Wnioskodawca** – administrator lub podmiot przetwarzający, który złożył wniosek o certyfikację swoich operacji przetwarzania;

16. **Klient** – podmiot, który uzyskał certyfikację (wcześniej Wnioskodawca).

§ 4.

Ogólne wymogi w zakresie akredytacji

4.1 Kwestie prawne i umowne

4.1.1. Odpowiedzialność prawna

1. Podmiot certyfikujący musi zawsze być w stanie wykazać PCA, że posiada aktualne procedury potwierdzające przestrzeganie obowiązków prawnych określonych w warunkach akredytacji, w tym w dodatkowych wymogach dotyczących stosowania RODO.

2. Podmiot certyfikujący musi być w stanie wykazać, że jego procedury i środki dotyczące w szczególności kontroli i przetwarzania danych osobowych Wnioskodawcy i organizacji Klientów w ramach procesu certyfikacji są zgodne z RODO i u.o.d.o. W związku z tym, w ramach procedury akredytacji, Podmiot certyfikujący ma obowiązek przedstawić dowody zgodności wymagane w trakcie procesu akredytacji.

3. Do dowodów zgodności, o których mowa w pkt 2, należy w szczególności wykazanie przez Podmiot certyfikujący, że w/w procedury i środki stosowane w ramach procesu certyfikacji nie są i nie były w przeszłości przedmiotem postępowania przed Organem nadzorczym.

4. Przed przystąpieniem do procesu akredytacji PCA kontaktuje się z Organem nadzorczym w celu sprawdzenia informacji, o których mowa w pkt 3. W stosownych przypadkach Organ nadzorczy weryfikuje te informacje.

5. Podmiot certyfikujący potwierdza również PCA, że wdrożone i stosowane przez niego procedury i środki dotyczące w szczególności kontroli i przetwarzania danych osobowych Wnioskodawców i organizacji Klientów w ramach procesu certyfikacji nie są i nie były przedmiotem postępowań prowadzonych przez inne organy nadzorcze w innych sektorach, jeżeli te postępowania dotyczą przetwarzania

danych osobowych i mogą skutkować niespełnieniem tego wymogu przez Podmiot certyfikujący, a zatem mogą uniemożliwić jego akredytację.

6. Podmiot certyfikujący niezwłocznie informuje PCA o naruszeniach RODO lub u.o.d.o. stwierdzonych przez Organ nadzorczy, organy nadzorcze w innych sektorach lub właściwe organy wymiaru sprawiedliwości, które mogą mieć wpływ na jego akredytację.

7. Przed wydaniem lub odnowieniem lub odmową dokonania certyfikacji, Podmiot certyfikujący jest zobowiązany do poinformowania Organu nadzorczego zgodnie z art. 43 ust. 1 RODO i art. 19 u.o.d.o.

8. Organ nadzorczy może ustanowić dalsze wymogi i procedury w celu sprawdzenia zgodności podmiotów certyfikujących z RODO przed akredytacją.

4.1.2. Umowa o certyfikację

Oprócz wymogów ISO/IEC 17065/2012, Podmiot certyfikujący ma obowiązek wykazać, że jego umowa o certyfikację, o której mowa w art. 15 ust. 3 u.o.d.o.:

1. zobowiązuje Wnioskodawcę, aby zawsze spełniał zarówno ogólne wymogi certyfikacyjne w rozumieniu pkt 4.1.2.2 lit. a) ISO/IEC 17065/2012, jak i kryteria zatwierdzone przez Organ nadzorczy lub EROD zgodnie z art. 43 ust. 2 lit. b) i art. 42 ust. 5 RODO,

2. zobowiązuje Wnioskodawcę, aby zapewnił pełną przejrzystość wobec Organu nadzorczego w odniesieniu do procedury certyfikacji, w tym kwestii objętych postanowieniami umownymi o poufności, dotyczących ochrony danych, zgodnie z art. 42 ust. 7 i art. 58 ust. 1 lit. c) RODO,

3. nie ogranicza odpowiedzialności Wnioskodawcy za zgodność z RODO i pozostaje bez uszczerbku dla zadań i uprawnień organów nadzorczych, które są właściwe zgodnie z art. 42 ust. 5 RODO,

4. zobowiązuje Wnioskodawcę do dostarczenia Podmiotowi certyfikującemu wszelkich informacji i dostępu do jego czynności przetwarzania, które są niezbędne do

przeprowadzenia procedury certyfikacji zgodnie z art. 42 ust. 6 RODO,

5. zobowiązuje Wnioskodawcę do przestrzegania obowiązujących terminów i procedur - umowa o certyfikację musi przewidywać odpowiednie terminy i procedury, do przestrzegania których zostanie zobowiązany Wnioskodawca, program certyfikacji i inne przepisy muszą być monitorowane i przestrzegane,

6. w odniesieniu do pkt 4.1.2.2 lit. c) ppkt 1 ISO/IEC 17065/2012 - określa zasady ważności, odnowienia i wycofania zgodnie z art. 42 ust. 7 i art. 43 ust. 4 RODO, w tym zasady określające odpowiednie odstępy czasu na ponowną ocenę lub przegląd (regularność) zgodnie z art. 42 ust. 7 RODO i punktem 7.9 niniejszych wymogów,

7. umożliwia Podmiotowi certyfikującemu ujawnienie Organowi nadzorczemu wszystkich informacji niezbędnych do przyznania certyfikacji zgodnie z, odpowiednio, art. 42 ust. 8 i art. 43 ust. 5 RODO,

8. zawiera przepisy dotyczące niezbędnych środków ostrożności w odniesieniu do rozpatrywania skarg w rozumieniu pkt 4.1.2.2 lit. c) ppkt 2 i lit. j) ISO/IEC 17065/2012, zawiera również wyraźne oświadczenia na temat struktury i procedury rozpatrywania skarg zgodnie z art. 43 ust. 2 lit. d) RODO,

9. oprócz minimalnych wymogów, o których mowa w pkt 4.1.2.2 ISO/IEC 17065/2012, wskazuje konsekwencje dla Klienta w sytuacji cofnięcia lub zawieszenia lub niewydania akredytacji dla Podmiotu certyfikującego. Klient musi być w szczególności poinformowany o warunkach mających zastosowanie do przeniesienia certyfikacji oraz o procedurze, którą zobowiązany jest przestrzegać w przypadku, gdy Podmiot certyfikujący podlega odmowie, zawieszeniu lub decyzji o wycofaniu swojej akredytacji w odniesieniu do zatwierdzonego mechanizmu certyfikacji na mocy art. 42 RODO,

10. zobowiązuje Wnioskodawcę do poinformowania Podmiotu certyfikującego o ewentualnych istotnych zmianach jego sytuacji faktycznej lub prawnej oraz o zmianach produktów, procesów i usług objętych certyfikacją,

11. uwzględnia wiążące metody oceny w odniesieniu do przedmiotu oceny.

4.1.3. Stosowanie znaków jakości i oznaczeń w dziedzinie ochrony danych

Certyfikaty, pieczęcie i oznaczenia stosuje się wyłącznie zgodnie z art. 42 i 43 RODO oraz z Wytycznymi Rady dotyczącymi akredytacji i Wytycznymi Rady dotyczącymi certyfikacji.

4.2 Zarządzanie bezstronnością

PCA zapewnia, aby oprócz wymogu określonego w pkt 4.2 ISO/IEC 17065/2012:

1. Podmiot certyfikujący spełniał dodatkowe wymogi Organu nadzorczego (zgodnie z art. 43 ust. 1 lit. b) RODO):

   a) zgodnie z art. 43 ust. 2 lit. a) RODO Podmiot certyfikujący musi przedstawić odrębne dowody swojej niezależności. Dotyczy to w szczególności dowodów dotyczących finansowania Podmiotu certyfikującego w zakresie, w jakim dotyczy ono zapewnienia bezstronności,

   b) zadania i obowiązki Podmiotu certyfikującego nie prowadzą do konfliktu interesów zgodnie z art. 43 ust. 2 lit. e) RODO,

2. Podmiot certyfikujący nie miał żadnego istotnego związku z ocenianym Klientem (np. Podmiot certyfikujący nie może należeć do tej samej grupy przedsiębiorstw, Podmiot certyfikujący nie może być w żaden sposób kontrolowany przez Klienta, którego ocenia). Wszelkie powiązania gospodarcze między Podmiotem certyfikującym a Wnioskodawcą, w zależności od jego cech mogą wpływać na bezstronność jego działalności certyfikacyjnej.

4.3 Odpowiedzialność i finansowanie

Oprócz wymogu określonego w pkt 4.3.1 ISO/IEC 17065/2012 PCA regularnie zapewnia, aby Podmiot certyfikujący dysponował odpowiednimi środkami (np. ubezpieczeniem lub rezerwami) w celu pokrycia swoich zobowiązań w regionach geograficznych, w których prowadzi działalność.

4.4 Niedyskryminujące warunki

Stosuje się wymagania normy ISO/IEC 17065/2012.

4.5 Poufność

Stosuje się wymagania normy ISO/IEC 17065/2012.

4.6 Informacje dostępne publiczne

Oprócz wymogu określonego w pkt 4.6 ISO/IEC 17065/2012 PCA zobowiązuje Podmiot certyfikujący co najmniej do tego, aby:

1. wszystkie wersje (obecne i poprzednie) zatwierdzonych kryteriów zastosowanych w rozumieniu art. 42 ust. 5 RODO (kryteriów certyfikacji) były publikowane i łatwo dostępne publicznie, a także wszystkie procedury certyfikacji, z ogólnym wskazaniem odpowiedniego okresu ważności;

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

§ 5.

Wymogi strukturalne, art. 43 ust. 4 RODO

(właściwa ocena)

5.1 Struktura organizacyjna i ścisłe kierownictwo

Stosuje się wymogi normy ISO/IEC 17065/2012.

5.2 Mechanizmy zapewnienia bezstronności

Stosuje się wymogi normy ISO/IEC 17065/2012.

§ 6.

Wymogi dotyczące zasobów

6.1 Personel podmiotu certyfikującego

Oprócz wymogu zawartego w sekcji 6 normy ISO/IEC 17065/2012 PCA zapewnia w odniesieniu do każdego Podmiotu certyfikującego, aby jego personel wykonujący zadania związane ze zgodnością z certyfikacją:

1. wykazał się odpowiednią i bieżącą wiedzą fachową i doświadczeniem w zakresie ochrony danych zgodnie z art. 43 ust. 1 RODO,

2. posiadał niezależność i aktualną wiedzę fachową w odniesieniu do przedmiotu certyfikacji zgodnie z art. 43 ust. 2 lit. a) RODO i nie ma konfliktu interesów zgodnie z art. 43 ust. 2 lit. e) RODO,

3. zobowiązał się do przestrzegania kryteriów, o których mowa w art. 42 ust. 5, zgodnie z art. 43 ust. 2 lit. b) RODO,

4. posiadał odpowiednią wiedzę i doświadczenie na temat stosowania przepisów o ochronie danych,

5. posiadał odpowiednią wiedzą i doświadczenie w zakresie technicznych i organizacyjnych środków ochrony danych,

6. był w stanie wykazać doświadczenie w dziedzinach wymienionych w pkt 6.1 ppkt 1, 4 i 5, w szczególności:

   a) pracownicy posiadający fachową wiedzę techniczną:

      – uzyskali kwalifikacje w odpowiednim obszarze specjalistycznej wiedzy technicznej co najmniej na poziomie 6 według europejskich ram kwalifikacji lub uznanego chronionego tytułu (np. dyplom inżynierski) w danym zawodzie regulowanym lub muszą posiadać znaczące doświadczenie zawodowe,

      – dodatkowo pracownicy odpowiedzialni za decyzje certyfikacyjne muszą posiadać znaczące doświadczenie zawodowe w zakresie prawa ochrony danych, w tym w określaniu i wdrażaniu środków ochrony danych lub dostępu do osoby posiadającej tę wiedzę oraz odpowiednie kwalifikacje zawodowe/wykształcenie na poziomie podyplomowym,

      – dodatkowo pracownicy odpowiedzialni za oceny muszą posiadać doświadczenie zawodowe w zakresie technicznych środków ochrony danych oraz wiedzę i doświadczenie w zakresie porównywalnych procedur (np. certyfikacji/audytów), a w stosownych przypadkach wykazać rejestrację.

   Pracownicy ci muszą wykazać, że utrzymują wiedzę specjalistyczną w zakresie umiejętności technicznych i audytowych poprzez ustawiczne doskonalenie zawodowe.

b) pracownicy posiadający fachową wiedzę prawniczą:

- mają ukończone studia prawnicze na uczelni uznanej na szczeblu unijnym lub krajowym, trwające co najmniej osiem semestrów i zakończone uzyskaniem stopnia magistra prawa lub równoważnego stopnia, bądź posiadają znaczące doświadczenie zawodowe,

- dodatkowo pracownicy odpowiedzialni za decyzje certyfikacyjne muszą wykazać się znaczącym doświadczeniem zawodowym w zakresie prawa ochrony danych, w tym określania i wdrażania środków ochrony danych i być zarejestrowani zgodnie z wymogami państwa członkowskiego,

- dodatkowo pracownicy odpowiedzialni za oceny muszą wykazać posiadanie co najmniej dwuletniego doświadczenia zawodowego w zakresie prawa ochrony danych oraz wiedzy i doświadczenia w zakresie porównywalnych procedur (np. certyfikacji/audytów), oraz być zarejestrowani, o ile jest to wymagane przez dane państwo członkowskie.

    - Pracownicy muszą wykazać, że utrzymują wiedzę specjalistyczną w zakresie umiejętności technicznych i audytowych poprzez ustawiczne doskonalenie zawodowe.

Podmiot certyfikujący musi być w stanie określić i wyjaśnić PCA, które wymogi dotyczące doświadczenia zawodowego i wiedzy specjalistycznej są odpowiednie do zakresu systemu certyfikacji i danego przedmiotu oceny.

Podmiot certyfikujący jest odpowiedzialny za podejmowanie decyzji nawet jeżeli korzysta z pomocy podwykonawców.

Podwykonawcy nie mogą być zaangażowani w procesy decyzyjne.

Podwykonawcy muszą spełniać wymogi określone dla personelu Podmiotu certyfikującego.

6.2 Zasoby na potrzeby oceny

Stosuje się wymagania normy ISO/IEC 17065/2012.

§ 7.

Wymogi dotyczące procesów, art. 43 ust. 2 lit. c) i d) RODO

7.1 Wytyczne ogólne

Oprócz wymogu określonego w sekcji 7.1 ISO/IEC 17065/2012 PCA zapewnia aby:

1. przy składaniu wniosku Podmioty certyfikujące spełniały niniejsze dodatkowe wymogi Organu nadzorczego (zgodnie z art. 43 ust. 1 lit. b) RODO), tak aby zadania i obowiązki realizowane w związku z udzielaniem akredytacji nie prowadziły do konfliktu interesów zgodnie z art. 43 ust. 2 lit. e) RODO;

2. jeżeli Podmiot certyfikujący zamierza działać w innych państwach członkowskich za pośrednictwem biura pomocniczego (jednostki organizacyjnej, np. oddział czy spółkę zależną) powiadamia o tym odpowiednie właściwe organy i w razie potrzeby uzyskuje niezbędną zgodę, w tym na funkcjonowanie europejskiej pieczęci ochrony danych zgodnie z art. 42 ust. 5 RODO[3];

3. Podmioty certyfikujące posiadały procedury powiadamiania Organu nadzorczego bezpośrednio przed wydaniem, odnowieniem lub wycofaniem certyfikacji oraz podawały powody podjęcia takich działań. Obejmuje to dostarczenie Organowi nadzorczemu kopii streszczenia sprawozdania z oceny, o którym mowa w pkt 7.8 niniejszego dokumentu;

4. w przypadku, gdy Klient lub Organ nadzorczy powiadamia Podmioty certyfikujące o wszelkich istotnych postępowaniach lub działaniach regulacyjnych Organu nadzorczego lub innych organów nadzorczych w innych sektorach, powiązanych z zakresem certyfikacji i przedmiotem oceny, które podważają przestrzeganie przez Klienta ochrony danych, Podmioty certyfikujące są zobowiązane do dokonania oceny, czy Klient nadal spełnia kryteria certyfikacji. Podmioty certyfikujące przekażą Organowi nadzorczemu sprawozdanie zawierające informacje na temat wyników tej oceny. Ocena będzie związana z zakresem certyfikacji i zakresem przedmiotu oceny.

[3] W tym względzie zob. Wytyczne Rady dotyczące certyfikacji, pkt 44

7.2 Wniosek

Oprócz wymogów określonych w art. 17 u.o.d.o. oraz w punkcie 7.2 normy ISO/IEC 17065/2012 Podmiot certyfikujący wymaga, aby wniosek o udzielenie certyfikacji:

1. zawierał szczegółowy opis przedmiotu oceny, obejmuje to również interfejsy i transfery do innych systemów i organizacji, protokoły i inne gwarancje;

2. określał, czy Wnioskodawca korzysta z usług podmiotów przetwarzających, a jeżeli Wnioskodawcą jest podmiot przetwarzający – muszą w nim zostać opisane obowiązki i zadania, a do wniosku musi zostać załączona umowa lub umowy między administratorem a podmiotem przetwarzającym (kopie potwierdzone za zgodność);

3. określał, czy współadministratorzy są zaangażowani w przetwarzanie danych osobowych oraz czy współadministrator jest Wnioskodawcą – w takiej sytuacji we wniosku opisuje się jego obowiązki i zadania, a do wniosku musi zostać załączona umowa o współadministrowanie (kopia potwierdzona za zgodność);

4. ujawniał wszelkie bieżące lub niedawne postępowania lub działania regulacyjne prowadzone przez Organ nadzorczy lub organy nadzorcze w innych sektorach, którym podlega Wnioskodawca, jeżeli te postępowania lub działania regulacyjne dotyczą przetwarzania danych osobowych związanych z zakresem certyfikacji i zakresem przedmiotu oceny.

Podmiot certyfikujący jest zobowiązany do poinformowania Organu nadzorczego o otrzymaniu wniosku w celu umożliwienia mu realizacji zadań wynikających z RODO i u.o.d.o.

7.3 Ocena wniosku

Oprócz wymogów określonych w punkcie 7.3 normy ISO/IEC 17065/2012 PCA wymaga, aby:

1. w umowie o certyfikację określone były wiążące metody oceny w odniesieniu do przedmiotu oceny,

2. w ocenie dotyczącej wystarczającej wiedzy fachowej, przewidzianej w pkt 7.3 lit. e) normy ISO/IEC 17065/2012,

uwzględniano w odpowiednim zakresie zarówno techniczną, jak i prawną wiedzę fachową w zakresie ochrony danych.

7.4 Ocena

Oprócz wymogów określonych w punkcie 7.4 normy ISO/IEC 17065/2012 mechanizmy certyfikacji muszą określać wystarczające metody oceny zgodności operacji przetwarzania z kryteriami certyfikacji, w tym takie obszary jak:

1. metodę oceny konieczności i proporcjonalności operacji przetwarzania w stosunku do ich celu i osób, których te dane dotyczą,

2. metodę oceny zakresu, składu i analizy wszystkich rodzajów ryzyka rozważanych przez administratorów i podmioty przetwarzające, w odniesieniu do skutków prawnych zgodnie z art. 30, 32, 35 i 36 RODO oraz w odniesieniu do definicji środków technicznych i organizacyjnych zgodnie z art. 24, 25 i 32 RODO, w zakresie, w jakim wyżej wymienione artykuły mają zastosowanie do przedmiotu certyfikacji,

3. metodę oceny środków zaradczych, w tym gwarancji, zabezpieczeń i procedur w celu zapewnienia ochrony danych osobowych w kontekście przetwarzania, które ma zostać przypisane przedmiotowi certyfikacji oraz wykazania, że wymogi prawne określone w przyjętych kryteriach są spełnione, oraz

4. sposób dokumentowania metod i ustaleń.

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

Oprócz wymogów określonych w punkcie 7.4.2 normy ISO/IEC 17065/2012 ocena może być przeprowadzona przez podwykonawców, którzy zostali uznani przez Podmiot certyfikujący, z zastosowaniem tych samych wymogów dotyczących personelu określonych w § 6 niniejszego dokumentu.

Oprócz punktu 7.4.5 normy ISO 17065 należy przewidzieć, że istniejąca certyfikacja w zakresie ochrony danych zgodna z art. 42 i 43 RODO, która obejmuje już część przedmiotu oceny, może zostać

uwzględniona w ramach nowej oceny, ale nie będzie ona jednak wystarczająca, aby całkowicie zastąpić oceny częściowe. Sam certyfikat nie będzie jednak wystarczającym dowodem, a Podmiot certyfikujący jest zobowiązany do sprawdzenia zgodności z kryteriami w odniesieniu do przedmiotu oceny. W celu podjęcia świadomej decyzji uwzględnia się pełne sprawozdanie z oceny i inne istotne informacje umożliwiające ocenę istniejącej certyfikacji i jej wyników. Oświadczenie certyfikacyjne lub podobne świadectwa certyfikacji nie powinny być uznawane za wystarczające do zastąpienia sprawozdania.

W przypadkach, gdy istniejąca certyfikacja jest brana pod uwagę w ramach nowej oceny, zakres tej certyfikacji należy również szczegółowo ocenić pod kątem jej zgodności z odpowiednimi kryteriami certyfikacji.

W uzupełnieniu do pkt 7.4.6 normy ISO/IEC 17065/2012 Podmiot certyfikujący musi szczegółowo określić w swoim systemie certyfikacji, w jaki sposób informacje wymagane w tym punkcie normy ISO/IEC 17065/2012 pozwalają Klientowi (Wnioskodawcy) uzyskać wiedzę o niezgodnościach w odniesieniu do mechanizmu certyfikacji. W tym kontekście należy określić przynajmniej charakter i ramy czasowe takich informacji. Podmiot certyfikujący wykazuje to w pisemnym dokumencie, który może być systemem certyfikacji lub, jeżeli Podmiot certyfikujący nie jest właścicielem systemu, innym dokumentem odnoszącym się do procesu certyfikacji.

W uzupełnieniu do pkt 7.4.9 normy ISO/IEC 17065/2012 Podmiot certyfikujący zapewnia Organowi nadzorczemu pełny dostęp do dokumentacji z przeprowadzonej oceny Wnioskodawcy.

7.5 Przegląd

W uzupełnieniu do pkt 7.5 normy ISO/IEC 17065/2012 Podmiot certyfikujący określa procedury przyznawania, regularnego przeglądu i cofania odpowiednich certyfikatów zgodnie z art. 43 ust. 2 i 3 RODO.

Podmiot certyfikujący zapewnia Organowi nadzorczemu pełny dostęp do dokumentacji Klienta związanej z przyznawaniem, przeglądami i cofaniem certyfikatów.

7.6 Decyzja o certyfikacji

W uzupełnieniu do pkt 7.6.1 normy ISO/IEC 17065/2012, Podmiot certyfikujący jest zobowiązany do szczegółowego określenia w

swoich procedurach w jaki sposób zapewniono jego niezależność i odpowiedzialność w odniesieniu do poszczególnych decyzji certyfikacyjnych.

7.7 Dokumentacja certyfikacji

W uzupełnieniu do pkt 7.7.1 lit. e) normy ISO/IEC 17065/2012 oraz zgodnie z art. 42 ust. 7 RODO wymagane jest, aby okres ważności certyfikatów nie przekraczał trzech lat.

W uzupełnieniu do pkt 7.7.1 lit. e) normy ISO/IEC 17065/2012 wymagane jest również udokumentowanie okresu zamierzonego monitorowania w rozumieniu pkt 7.9 niniejszego dokumentu.

W uzupełnieniu do pkt 7.7.1 lit. f) normy ISO/IEC 17065/2012 Podmiot certyfikujący zobowiązany jest do wskazania przedmiotu certyfikacji w dokumentacji certyfikacji (z podaniem statusu wersji lub, w stosownych przypadkach, podobnych cech).

Przy wydawaniu certyfikatu Podmiot certyfikujący zobowiązany jest dostarczyć Organowi nadzorczemu kopię dokumentacji certyfikacji, o której mowa w normie ISO/IEC 17065/2012 pkt 7.7.1.

7.8 Wykaz certyfikowanych produktów

W uzupełnieniu do pkt 7.8 normy ISO/IEC 17065/2012 Podmiot certyfikujący zobowiązany jest do utrzymywania wewnętrznej i publicznej dostępności informacji na temat certyfikowanych produktów, procesów i usług.

Podmiot certyfikujący podaje do wiadomości publicznej streszczenie sprawozdania z oceny, służące zapewnieniu przejrzystości co do przedmiotu certyfikacji i sposobu oceny. W streszczeniu przedstawia się między innymi:

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

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

c) metody oceny i przeprowadzone badania,

d) wyniki.

W uzupełnieniu do pkt 7.8 normy ISO/IEC 17065/2012 i zgodnie z art. 43 ust. 5 RODO Podmiot certyfikujący informuje właściwe organy

nadzorcze o przyczynach udzielania lub cofnięcia lub odmowy certyfikacji, o którą się do niego zwrócono.

7.9 Nadzór

W uzupełnieniu do pkt 7.9.1, 7.9.2 i 7.9.3 normy ISO/IEC 17065/2012 oraz zgodnie z art. 43 ust. 2 lit. c) RODO wymaga się, aby w celu utrzymania certyfikacji w okresie monitorowania Podmiot certyfikujący określił środki regularnego monitorowania. Środki takie powinny być oparte na analizie ryzyka i proporcjonalne, a maksymalny okres między działaniami w zakresie nadzoru nie powinien przekraczać 12 miesięcy.

7.10 Zmiany mające wpływ na certyfikację

W uzupełnieniu do pkt 7.10.1 i 7.10.2 normy ISO/IEC 17065/2012 zmiany mające wpływ na certyfikację, które mają być uwzględnione przez Podmiot certyfikujący, obejmują:

1. każde naruszenie ochrony danych osobowych lub inne naruszenie RODO lub u.o.d.o. stwierdzonych przez Organ nadzorczy, organy nadzorcze w innych sektorach lub organy wymiaru sprawiedliwości, które dotyczy certyfikacji, zgłoszone przez Klienta lub Organ nadzorczy. Powyższe naruszenia są uwzględniane tylko w zakresie, w jakim odnoszą się do certyfikacji.

2. zmiany spowodowane nowymi osiągnięciami technologicznymi (w zakresie istotnym dla przyszłej certyfikacji i nadzoru),

3. zmiany w przepisach prawnych dotyczących ochrony danych osobowych,

4. przyjęcia aktów delegowanych Komisji Europejskiej zgodnie z art. 43 ust. 8 i art. 43 ust. 9 RODO,

5. decyzje, opinie, wytyczne, zalecenia, najlepsze praktyki lub inne dokumenty przyjęte przez Radę oraz

6. orzeczenia sądowe dotyczące ochrony danych.

Procedury zmian wprowadzane przez Podmiot certyfikujący obejmują takie kwestie jak: okresy przejściowe, proces zatwierdzania przez właściwy organ nadzorczy, ponowna ocena odpowiednich przedmiotów oceny oraz odpowiednie środki służące cofnięciu certyfikacji, jeżeli certyfikowana operacja przetwarzania nie spełnia już zaktualizowanych kryteriów.

7.11 Wygaśnięcie, ograniczenie, zawieszenie lub cofnięcie certyfikacji

W uzupełnieniu do pkt 7.11.1 normy ISO/IEC 17065/2012 oraz pkt 7.1 ppkt 3 niniejszego dokumentu, Podmiot certyfikujący jest zobowiązany do niezwłocznego pisemnego poinformowania Organu nadzorczego i w stosownych przypadkach PCA o podjętych środkach oraz o przedłużeniu, ograniczeniu, zawieszeniu i cofnięciu certyfikacji.

Zgodnie z art. 58 ust. 2 lit. h) RODO Podmiot certyfikujący jest zobowiązany do przyjęcia decyzji i nakazów Organu nadzorczego dotyczących cofnięcia lub odmowy wydania certyfikacji Klientowi (Wnioskodawcy), jeżeli wymóg certyfikacji nie jest lub przestał być spełniany.

7.12 Ewidencja

Oprócz wymogów normy ISO/IEC 17065/2012 Podmiot certyfikujący zobowiązany jest do przechowywania całej dokumentacji w formie kompletnej, zrozumiałej, aktualizowanej i nadającej się do przeprowadzenia audytu.

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

W uzupełnieniu do punktu 7.13.1 normy ISO/IEC 17065/2012, Podmiot certyfikujący zobowiązany jest określić:

a) kto może składać skargi lub zastrzeżenia,

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

c) jakie weryfikacje mają miejsce w tym kontekście oraz

d) możliwości konsultacji z zainteresowanymi stronami.

W uzupełnieniu do punktu 7.13.2 normy ISO/IEC 17065/2012, Podmiot certyfikujący zobowiązany jest określić:

a) w jaki sposób i komu należy wydać potwierdzenie, o którym mowa w pkt 7.13.2 normy ISO/IEC 17065/2012,

b) terminy w tym zakresie oraz

c) jakie procesy należy następnie uruchomić.

Podmioty certyfikujące są zobowiązane do publicznego udostępniania swoich procedur rozpatrywania skarg osobom, których dane dotyczą i zapewnienia im łatwego dostępu.

Podmiot certyfikujący jest zobowiązany do poinformowania skarżących w rozsądnym terminie o postępach i wyniku rozpatrywania skargi.

W uzupełnieniu do punktu 7.13.1 normy ISO/IEC 17065/2012 Podmiot certyfikujący musi określić, w jaki sposób zapewnia się rozdzielenie działań certyfikacyjnych od rozpatrywania odwołań i skarg.

§ 8.

Wymogi dotyczące systemu zarządzania

Ogólnym wymogiem systemu zarządzania zgodnie z rozdziałem 8 normy ISO/IEC 17065/2012 jest to, aby wdrożenie wszystkich wymogów z poprzednich rozdziałów w zakresie stosowania mechanizmu certyfikacji przez Podmiot certyfikujący było niezależnie dokumentowane, oceniane, kontrolowane i monitorowane.

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

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

Te zasady zarządzania i ich udokumentowane wdrażanie muszą być przejrzyste i ujawniane przez Podmiot certyfikujący w ramach procedury akredytacji zgodnie z art. 58 RODO, a następnie na wniosek Organu nadzorczego w każdym momencie podczas postępowania w formie przeglądów w zakresie ochrony danych na podstawie art. 58 ust. 1 lit. b) RODO lub przeglądu – na podstawie art. 58 ust. 1 lit. c) RODO – certyfikacji udzielonych na mocy art. 42 ust. 7 RODO.

Podmiot certyfikujący musi w szczególności stale podawać do wiadomości publicznej, które certyfikacje (lub mechanizmy, bądź systemy certyfikacji)

zostały przeprowadzone na jakiej podstawie oraz jaki jest okres ważności certyfikacji na podstawie jakich ram i warunków (motyw 100 RODO), niezależnie od obowiązku wynikającego z art. 23 u.o.d.o., czyli przekazania Organowi nadzorczemu danych podmiotu, któremu udzielono certyfikacji, oraz podmiotu, któremu cofnięto certyfikację, wraz ze wskazaniem przyczyny jej cofnięcia.

Procedury stosowane w przypadku zawieszenia lub cofnięcia akredytacji zostają włączone do systemu zarządzania Podmiotów certyfikujących, w tym do powiadamiania ich Klientów i Wnioskodawców.

Podmiot certyfikujący ustanawia proces rozpatrywania skarg z niezbędnymi poziomami niezależności jako integralną część systemu zarządzania, który w szczególności wdraża wymogi określone w pkt 4.1.2.2 lit. c) i j), 4.6 lit. d) i 7.13 normy ISO/IEC 17065/2012. Istotne skargi i zastrzeżenia należy zgłaszać Organowi nadzorczemu.

8.1 Ogólne wymogi dotyczące systemu zarządzania

Stosuje się wymagania normy ISO/IEC 17065/2012.

8.2 Dokumentacja systemu zarządzania

Stosuje się wymagania normy ISO/IEC 17065/2012.

8.3 Kontrola dokumentów

Stosuje się wymagania normy ISO/IEC 17065/2012.

8.4 Kontrola ewidencji

Stosuje się wymagania normy ISO/IEC 17065/2012.

8.5 Przegląd systemu zarządzania

Stosuje się wymagania normy ISO/IEC 17065/2012.

8.6 Audyty wewnętrzne

Stosuje się wymagania normy ISO/IEC 17065/2012.

8.7 Działania naprawcze

Stosuje się wymagania normy ISO/IEC 17065/2012.

8.8 Działania zapobiegawcze

Stosuje się wymagania normy ISO/IEC 17065/2012.

§ 9.

Dalsze dodatkowe wymogi

9.1 Aktualizacja oceny

Podmiot certyfikujący ustanawia procedury dotyczące aktualizacji metod oceny stosowanych w kontekście oceny zgodnie z pkt 7.4 normy ISO/IEC 17065/2012 i niniejszego dokumentu. Aktualizacja musi nastąpić w przypadku zmian ram prawnych, odnośnego ryzyka, aktualnego stanu wiedzy i kosztów wdrożenia środków technicznych i organizacyjnych.

9.2 Utrzymywanie wiedzy fachowej

Podmioty certyfikujące ustanawiają procedury zapewniające szkolenie swoich pracowników w celu aktualizacji ich umiejętności, uwzględniając zmiany wymienione w pkt 9.1 niniejszego dokumentu.

9.3 Zakresy odpowiedzialności i kompetencji

9.3.1 Komunikacja między Podmiotem certyfikującym a jego Klientami i Wnioskodawcami

Podmiot certyfikujący opracowuje odpowiednie procedury i struktury komunikacji między nim a Klientem/Wnioskodawcą. Obejmują one:

1. prowadzenie przez Podmiot certyfikujący dokumentacji podziału zadań i obowiązków do celów:
    a) odpowiadanie na wnioski o udzielenie informacji, lub
    b) umożliwienia kontaktu w przypadku skargi dotyczącej certyfikacji;
2. prowadzenie procesu przyjmowania wniosków w celu:
    a) udzielania informacji o postępie w rozpatrywaniu wniosku;
    b) przeprowadzania przez Organ nadzorczy oceny dotyczącej:
        – informacji zwrotnej;
        – decyzji Organu nadzorczego.

9.3.2 Dokumentacja działalności w zakresie oceny

Podmiot certyfikujący wprowadza systemy służące wdrażaniu odpowiednich procedur i struktur komunikacji między Podmiotem certyfikującym a Organem nadzorczym. Obejmuje to ramy sprawozdawczości w celu poinformowania Organu nadzorczego o:

1. szczegółowych informacjach dotyczących Wnioskodawcy, aby umożliwić Organowi nadzorczemu sprawdzenie czy w przeszłości był stroną postępowania przed Organem nadzorczym;

2. powodach udzielenia/cofnięcia certyfikacji zgodnie z art. 43 ust. 5 RODO bezpośrednio przed wydaniem, odnowieniem, zawieszeniem lub cofnięciem certyfikacji zgodnie z sekcją 7.1 ust. 3 niniejszego dokumentu.

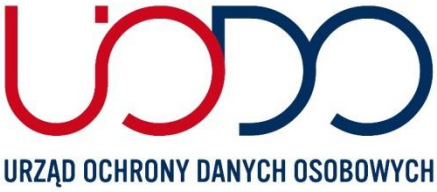
9.3.3 Zarzadzanie rozpatrywaniem skarg

Integralną część systemu zarządzania stanowi procedura rozpatrywania skarg, która musi być zgodna z wymogami pkt 4.1.2.2 lit. c) i j), 4.6 lit. d) i 7.13 normy ISO/IEC 17065/2012.

Podmiot certyfikujący zobowiązany jest zgłaszać Organowi nadzorczemu odpowiednie skargi i sprzeciwy.

9.3.4 Zarządzanie cofaniem akredytacji

Procedura stosowana w przypadku zawieszenia lub cofnięcia akredytacji stanowi część systemu zarządzania Podmiotu certyfikującego. Obejmuje ona również powiadamianie Klientów.



ul. Stawki 2

00-193 Warszawa

www.uodo.gov.pl