URZĄD OCHRONY DANYCH OSOBOWYCH

CERTYFIKACJA W OCHRONIE DANYCH OSOBOWYCH

PIOTR DROBEK

UODO, UKSW

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

MECHANIZMY CERTYFIKACJI – RAMY PRAWNE

URZĄD OCHRONY DANYCH OSOBOWYCH

- Art. 42 i 43 RODO
- Wytyczne Europejskiej Rady Ochrony Danych 1/2018 w sprawie certyfikacji i identyfikacji kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia Wersja 3.0
- Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation)
- Wytyczne Europejskiej Rady Ochrony Danych 4/2018 w sprawie akredytacji zgodnie z art. 43 RODO
- Wytyczne 07/2022 dotyczące certyfikacji jako narzędzia do przekazywania danych, Wersja 2.0, przyjęte 14 lutego 2023 r.
- Ustawa z 10.05.2018 r. o ochronie danych osobowych – art. 12-26
- Ustawa 13.04.2016 r. o systemach oceny zgodności i nadzoru rynku – rozdział 4 (z wyjątkiem art. 24 ust. 4–7 oraz art. 25 ust. 1 i 2 w zakresie dotyczącym ograniczenia zakresu akredytacji oraz jej zawieszenia)
- Dodatkowe wymogi akredytacji podmiotów certyfikujących z 8 grudnia 2023 r. Wersja 1.2

CEL CERTYFIKACJI

Zgodnie z art. 42 ust. 1 RODO mechanizmy certyfikacji ustanawia się, by świadczyły

„o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające”.

CEL CERTYFIKACJI

URZĄD OCHRONY DANYCH OSOBOWYCH

Zatwierdzone mechanizmy certyfikacji można wykorzystywać do wykazania wypełnienia zobowiązań przez administratorów i podmioty przetwarzające, które 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

CEL CERTYFIKACJI

URZĄD OCHRONY DANYCH OSOBOWYCH

- Za pomocą certyfikacji samej w sobie nie można udowodnić zgodności z przepisami.
- Certyfikacja stanowi 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.
- W dokumentacji musza zostać 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

PODSTAWOWE POJĘCIA

URZĄD OCHRONY DANYCH OSOBOWYCH

- Certyfikacja to „dostarczenie przez niezależny organ pisemnego zapewnienia (certyfikatu), że dany produkt, usługa lub system spełnia określone wymagania”. – ISO (definicja uniwersalna)
- „Zaświadczenie przez osobę trzecią (...) związane z produktami, procesami i usługami”. - norma EN-ISO/IEC 17000:2004 – Ocena zgodności – Słownictwo i ogólne zasady (do których odwołuje się norma ISO17065)

PODSTAWOWE POJĘCIA

URZĄD OCHRONY DANYCH OSOBOWYCH

- Certyfikacja to ocena zgodności przez stronę trzecią
- Podmiot certyfikujący – jednostka oceniająca zgodność

PODSTAWOWE POJĘCIA

URZĄD OCHRONY DANYCH OSOBOWYCH

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

MECHANIZMY CERTYFIKACJI, ZNAKI JAKOŚCI I OZNACZENIA

URZĄD OCHRONY DANYCH OSOBOWYCH

- 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.

CERTYFIKAT, ZNAKI JAKOŚCI I OZNACZENIA

URZĄD OCHRONY DANYCH OSOBOWYCH

- 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.

KTO MOŻE UDZIELAĆ CERTYFIKACJI?

URZĄD OCHRONY DANYCH OSOBOWYCH

- Organ nadzorczy
- Akredytowany podmiot certyfikujący

RODZAJE MECHANIZMÓW CERTYFIKACJI?

URZĄD OCHRONY DANYCH OSOBOWYCH

- Europejski znak jakości ochrony danych
- Krajowe machanizmy certyfikacji

ROLA ORGANÓW NADZORCZYCH

URZĄD OCHRONY DANYCH OSOBOWYCH

- 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;
- może zachęcać rynek do tworzenia mechanizmów certyfikacji.

ROLA ORGANÓW NADZORCZYCH

URZĄD OCHRONY DANYCH OSOBOWYCH

- ocena kryteriów systemu certyfikacji oraz przygotowanie projektu decyzji (art. 42 ust. 5);
- przekazanie EROD projektu decyzji, kiedy Rada 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));

ROLA ORGANÓW NADZORCZYCH

URZĄD OCHRONY DANYCH OSOBOWYCH

- 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).

KRYTERIA CERTYFIKACJI

URZĄD OCHRONY DANYCH OSOBOWYCH

RODO powierza organom nadzorczym zadanie polegające na zatwierdzaniu kryteriów certyfikacji,

ale nie na opracowywaniu tych kryteriów.

PRZEDMIOT CERTYFIKACJI

URZĄD OCHRONY DANYCH OSOBOWYCH

Zakres certyfikacji na podstawie RODO jest ukierunkowany na operacje przetwarzania lub zestawy operacji.

PRZEDMIOT CERTYFIKACJI

URZĄD OCHRONY DANYCH OSOBOWYCH

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.

PRZEDMIOT CERTYFIKACJI

URZĄD OCHRONY DANYCH OSOBOWYCH

Zakres mechanizmu certyfikacji – może być określony w sposób ogólny lub w odniesieniu do konkretnego rodzaju lub obszaru operacji przetwarzania.

Przedmiot certyfikacji (przedmiot oceny) w poszczególnych projektach certyfikacyjnych.

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.

OPINIE EROD W SPRAWIE KRYTERIÓW CERTYFIKACJI

URZĄD OCHRONY DANYCH OSOBOWYCH

- Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria
- Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors
- **Opinia 28/2022 w sprawie kryteriów certyfikacji Europrivacy dotycząca ich zatwierdzenia przez Radę jako europejskiego znaku jakości ochrony danych zgodnie z art. 42 ust. 5 (RODO), przyjęta 10.10.2022 r.**
- Opinion 15/2023 on the draft decision of the Dutch Supervisory Authority regarding the Brand Compliance certification criteria, Adopted on 19 09 2023

URZĄD OCHRONY DANYCH OSOBOWYCH

DZIĘKUJĘ ZA UWAGĘ!

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl