Certyfikacja i kodeksy postępowania – podobieństwa i różnice

Posted on 2024-03-29

Przystąpienie do kodeksu postępowania lub otrzymanie certyfikatu dla konkretnego procesu przetwarzania danych jest dla klientów i partnerów biznesowych sygnałem,że podmiot w sposób odpowiedzialny podchodzi do ochrony danych osobowych i spełnia określone w RODO wymagania.

Zarówno kodeksy postępowania, jak i certyfikacja to przewidziane w RODO narzędzia służące wykazywaniu zgodności z rozporządzeniem. O podobieństwach i różnicach między nimi dyskutowano podczas trzeciego webinarium z serii „Certyfikacja w ochronie danych".

W grudniu 2023 r. Prezes UODO zatwierdził i opublikował na stronie internetowej Urzędu Dodatkowe wymogi akredytacji podmiotów certyfikujących. Obecnie trwa akcja edukacyjna, której celem jest zachęcanie rynku do tworzenia mechanizmów certyfikacji w zakresie ochrony danych osobowych zgodnie z art. 42 RODO. Ma ona formę cyklu webinariów „Certyfikacja w ochronie danych". Dotychczas odbyły się trzy spotkania poświęcone tej tematyce (12.12.2023 r., 30.01.2024 r. oraz 26.02.2024 r.), a nagraniaz ich przebiegu udostępnione są na stronie internetowej UODO. – Dotychczas w większości państw członkowskich nie zgromadzono szerokich doświadczeń związanych z certyfikacją w dziedzinie ochrony danych osobowych. Dlatego po rozpoczęciu stosowania rozporządzenia ogólnego przed pięcioma laty bardzo ważne było wypracowanie na poziomie europejskim

dodatkowych ram prawnych i organizacyjnych. Powinny one – dzięki dopracowaniu i rozwinięciu przede wszystkim art. 42 i 43 RODO umożliwić spójne stosowanie tego instrumentu w całej Unii Europejskiej – mówił w wystąpieniu otwierającym lutowe webinarium Mirosław Wróblewski, Prezes Urzędu Ochrony Danych Osobowych. Jak dodał, dzisiaj takie ramy już mamy, a tworzą je m.in. zatwierdzone przez Prezesa UODO Dodatkowe wymogi akredytacji podmiotów certyfikujących

W części głównej spotkania specjaliści UODO, wychodząc naprzeciw oczekiwaniom uczestników styczniowego webinarium, omówili najważniejsze cechy kodeksów postępowania i certyfikacji, podkreślając zwłaszcza ich zalety i wskazując różnice. Na potrzeby niniejszej publikacji Wydział Kodeksów i Certyfikacji w Departamencie Orzecznictwa i Legislacji przygotował zestawienie omawianych treści w formie tabeli.

Kodeksy postępowania i certyfikacja – porównanie narzędzi

W części głównej spotkania specjaliści UODO, wychodząc naprzeciw oczekiwaniom uczestników styczniowego webinarium, omówili najważniejsze cechy kodeksów postępowania i certyfikacji, podkreślając zwłaszcza ich zalety i wskazując różnice. Na potrzeby niniejszej publikacji Wydział Kodeksów i Certyfikacji w Departamencie Orzecznictwa i Legislacji przygotował zestawienie omawianych treści w formie tabeli.

Kryterium porównawcze	Kodeks postępowania	Certyfikacja

Definicje	Brak definicji „kodeksu postępowania” w RODO[1], u.o.d.o. [2] Kodeks postępowania to zbiór instrukcji dla administratorów danych i podmiotów przetwarzających (p. 7 Wytycznych 1/2019[3])	Brak definicji „certyfikacji” w RODO, u.o.d.o. 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 (p. 18 Wytycznych 1/2018[4]).
Funkcja, cel	Ma pomóc we właściwym stosowaniu RODO. Doprecyzowuje zastosowanie RODO (art. 40 ust. 1 i 2 RODO). Stanowi mechanizm umożliwiający wykazywanie zgodności z RODO (art. 24 ust. 3, art. 28 ust. 5, art. 32 ust. 3, art. 46 ust. 2 lit. e RODO).	Pozwala osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi (motyw 100 RODO). Ma świadczyć o zgodności z RODO operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające (art. 42 ust. 1 RODO). Stanowi mechanizm umożliwiający wykazywanie zgodności z RODO (art. 24 ust. 3, art. 28 ust. 5, art. 32 ust. 3, art. 46 ust. 2 lit. f RODO).

[1] 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 04.05.2016, str. 1, ze zm.).

[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781).

[3] Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679. Wersja 2.0, 4 czerwca 2019 r. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_pl

[4] Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia. Wersja 3.0, 4 czerwca 2019 r. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_pl

Kto może opracować	Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające (art. 40 ust. 2 RODO). Przykłady ww. podmiotów – p. 21-22 Wytycznych 1/2019.	RODO nie przewiduje ograniczeń w tym zakresie. Warto zwrócić uwagę na p. 2 procedury zatwierdzania kryteriów certyfikacji przez EROD[5].

Proces opracowania i zatwierdzania	Wniosek o zatwierdzenie kodeksu postępowania oraz jego projekt muszą być przygotowane z uwzględnieniem art. 40 RODO, art. 27 u.o.d.o. oraz p. 19 – 59 Wytycznych 1/2019. Kodeks krajowy – oznacza kodeks, który obejmuje czynności przetwarzania prowadzone w obrębie jednego państwa członkowskiego. Kodeks transgraniczny – oznacza kodeks, który obejmuje czynności przetwarzania prowadzone w więcej niż jednym państwie członkowskim. Prezes UODO zatwierdza kodeks postępowania w formie decyzji administracyjnej (art. 40 RODO, art. 27 i art. 7 u.o.d.o. oraz Kpa[6]).	Wskazówki dot. opracowywania mechanizmów certyfikacji znajdują się w dokumentach wydanych przez EROD – ich katalog jest dostępny na stronie UODO w zakładce Certyfikacja. Kryteria certyfikacji, stanowiące integralną część mechanizmu certyfikacji, są zatwierdzane odpowiednio przez organ nadzorczy (krajowy lub wielonarodowy mechanizm certyfikacji) lub EROD (ogólnoeuropejski mechanizm certyfikacji) (art. 42 ust. 5 RODO). Przed zatwierdzeniem kryteriów certyfikacji przez organ nadzorczy wymagana jest opinia EROD (art. 64 ust. 1 lit. c RODO). Zatwierdzanie kryteriów certyfikacji przez Prezesa UODO będzie miało formę decyzji administracyjnej (art. 42, art. 58 ust. 3 lit. f i ust. 4 RODO, Kpa) Wniosek o zatwierdzenie kryteriów certyfikacji przez EROD składa się do właściwego organu nadzorczego.

Kto może przystąpić do kodeksu/ uzyskać certyfikat	Administratorzy/podmioty przetwarzające: •podlegający RODO, •niepodlegający RODO (art. 40 ust. 3 RODO).Okres członkostwa w kodeksie uzależniony jest od woli członka kodeksu i przestrzegania kodeksu.	Administratorzy/podmioty przetwarzające: •podlegający RODO, •niepodlegający RODO. (art. 42 ust. 1 i 2 RODO) Certyfikat jest przyznawany na okres 3 lat, z możliwością jego przedłużenia lub cofnięcia (art. 42 ust. 7 RODO).

[5] EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals

https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-adoption-edpb-opinions-regarding_pl

[6] Ustawa z 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2023 r. poz. 775, ze zm.)

Terytorialny obszar obowiązywania	Państwo EOG, w którym kodeks został zatwierdzony przez organ nadzorczy, np. w Polsce – kodeks zatwierdzony przez Prezesa UODO. Kodeks transgraniczny i kodeks stanowiący odpowiednie zabezpieczenie w rozumieniu art. 46 ust. 2 lit. e RODO może stać się powszechnie obowiązujący w EOG (art. 40 ust. 9 i 10 RODO).	Państwo EOG, w którym zostały zatwierdzone kryteria certyfikacji. Państwa EOG, w których zostały zatwierdzone kryteria certyfikacji. EOG – w przypadku mechanizmu certyfikacji, którego kryteria certyfikacji zostały zatwierdzone przez EROD.

Akredytacja: podmiotu monitorującego przestrzeganie kodeksu/ podmiotu certyfikującego	Monitorowanie przestrzegania kodeksu postępowania dla podmiotów prywatnych to obowiązek akredytowanego podmiotu monitorującego. Podmiot monitorujący jest akredytowany przez Prezesa UODO do konkretnego kodeksu postępowania – Wymogi akredytacji podmiotów monitorujących kodeksy postępowania. Akredytacja jest udzielana na 5 lat, z możliwością jej cofnięcia. (art. 41 RODO, art. 29-32 u.o.d.o., Kpa). Prezes UODO prowadzi publicznie dostępny wykaz podmiotów akredytowanych (art. 33 u.o.d.o.).	Certyfikacja może być udzielana przez organ nadzorczy lub akredytowany podmiot certyfikujący (art. 42 ust. 5 RODO). Postępowanie akredytacyjne podmiotu certyfikującego prowadzone będzie w Polsce przez Polskie Centrum Akredytacji (art. 43 ust. 1 lit. b RODO, art. 12 ust. 1 u.o.d.o.). Akredytacja będzie dokonywana na podstawie normy EN-ISO/IEC 17065/2012 i Dodatkowych wymogów akredytacji podmiotów certyfikujących. Akredytacja jest udzielana na 5 lat, z możliwością jej przedłużenia lub cofnięcia (art. 43 ust. 4 i 7 RODO).
Czas obowiązywania	RODO nie określa okresu czasu obowiązywania kodeksu postępowania. Wymagane są procedury regularnego przeglądu treści kodeksu (art. 41 ust. 2 lit. b RODO).	RODO nie określa okresu czasu ważności mechanizmu certyfikacji. Wymagane są procedury regularnego przeglądu treści kryteriów certyfikacji (p. 75 Wytycznych 1/2018; sekcja 9 Dodatek do Wytycznych 1/2018[7]).

[7] 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) https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidance-certification-criteria-assessment_pl

Publiczny dostęp do treści: zatwierdzonego kodeksu/zatwierdzonych kryteriów certyfikacji	Prezes UODO ma obowiązek publikacji zatwierdzonego kodeksu postępowania (art. 40 ust. 6 RODO, art. 53 ust. 1 p. 2 u.o.d.o.). Rejestr wszystkich zatwierdzonych kodeksów postępowania jest prowadzony przez EROD (art. 40 ust. 11 RODO).	Prezes UODO ma obowiązek udostępnienia zatwierdzonych kryteriów certyfikacji (art. 43 ust. 6 RODO, art. 16 u.o.d.o.). EROD gromadzi w rejestrze wszystkie mechanizmy certyfikacji (art. 42 ust. 8 RODO).
Koszty	Koszty uzyskania statusu członka kodeksu i dalszego monitorowania przestrzegania kodeksu (tylko dla członków z sektora prywatnego) ustalają akredytowane podmioty monitorujące – dla zobrazowania: cennik RS Jamano sp. z o.o. sp.k. i KPMG Advisory sp. z o.o. sp. k.	Koszt certyfikacji, która będzie udzielana przez podmiot certyfikujący, nie jest jeszcze znany. W przypadku certyfikacji, która może być udzielana przez Prezesa UODO, jej maksymalny koszt został określony w art. 26 u.o.d.o.
Potwierdzenie członkostwa w kodeksie / uzyskania certyfikacji	RODO nie przewiduje żadnego dokumentu, który potwierdzałby członkostwo w kodeksie. Z dotychczas zatwierdzonych przez Prezesa UODO kodeksów postępowania wynika, że promowanie członkostwa w kodeksie odbywa się przez podanie do publicznej wiadomości informacji o uzyskaniu statusu podmiotu przestrzegającego kodeks przez twórcę kodeksu, podmiot monitorujący i samego zainteresowanego[8].	Certyfikat (art. 21 u.o.d.o.) Wykaz podmiotów, które uzyskały certyfikat lub go im cofnięto prowadzony przez Prezesa UODO (art. 23 u.o.d.o.).
Zasady monitorowania	Zarówno kodeks dla podmiotów prywatnych, jak i publicznych musi zawierać mechanizmy monitorowania przestrzegania jego postanowień (p. 88 Wytycznych 1/2019). Monitorowanie przestrzegania kodeksu przez podmioty prywatne prowadzi akredytowany podmiot monitorujący, który jest zobowiązany posiadać odpowiednie procedury w tym zakresie, które są przedmiotem postępowania akredytacyjnego (art. 41 ust. 2 lit. b RODO). Dla przykładu, mechanizm monitorowania przestrzegania kodeksu przez jego członków z sektora publicznego został opisany w p. 7.3 Kodeksu postępowania dla sektora ochrony zdrowia[9].	Z RODO wynika wymóg posiadania przez podmiot certyfikujący procedur okresowego przeglądu i cofania certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych (art. 43 ust. 2 lit. c RODO).

[8] Np. p. 7.3.11.1 Kodeks postępowania dla sektora ochrony zdrowia (PFSz) https://uodo.gov.pl/pl/426/1110

[9] Kodeks postępowania dla sektora ochrony zdrowia (PFSz) https://uodo.gov.pl/pl/426/1110

Utrata statusu członka kodeksu/certyfikatu	Akredytowany podmiot monitorujący podejmuje odpowiednie działania w przypadku naruszenia kodeksu przez administratora lub podmiot przetwarzający, w tym zawiesza go lub wyklucza spośród stosujących kodeks. O działaniach tych i powodach ich podjęcia informuje on właściwy organ nadzorczy (art. 41 ust. 4 RODO).	Akredytowany podmiot certyfikujący cofa certyfikację w przypadku stwierdzenia, że podmiot, któremu udzielono certyfikacji, nie spełnia lub przestał spełniać kryteria certyfikacji (art. 42 ust. 7 RODO, art. 22 u.o.d.o.).

Przystąpienie do kodeksu postępowania lub otrzymanie certyfikatu dla konkretnego procesu przetwarzania danych będzie dla klientów i partnerów biznesowych sygnałem, że podmiot mający status członka kodeksu lub dysponujący certyfikatem w sposób odpowiedzialny podchodzi do ochrony danych osobowych i spełnia określone w RODO wymagania. Jednocześnie stosowanie zatwierdzonych kodeksów postępowania lub mechanizmów certyfikacji będzie brane pod uwagę przy podejmowaniu przez Prezesa UODO decyzji o ewentualnym nałożeniu administracyjnej kary pieniężnej i jej wysokości (art. 83 ust. 2 lit. j RODO).

Webinarium było także okazją do przedstawienia kodeksów postępowania zatwierdzonych przez Prezesa UODO oraz omówienia współpracy z inicjatywami pracującymi nad kodeksami. Prowadzący spotkanie zachęcili do zapoznania się z treściami publikowanymi w zakładce Kodeksy postępowania oraz w zakładce Certyfikacja na stronie internetowej UODO. Poinformowali także, gdzie na stronie EROD szukać rejestru zatwierdzonych w EOG kodeksów postępowania oraz rejestru wszystkich zatwierdzonych mechanizmów certyfikacji.

Podczas webinarium wskazano także, że wszystkie podmioty zainteresowane opracowaniem kodeksu postępowania lub mechanizmu certyfikacji, czy uzyskaniem statusu akredytowanego podmiotu monitorującego kodeks lub akredytowanego podmiotu certyfikującego proszone są o kontakt z Wydziałem Kodeksów i Certyfikacji

(dol@uodo.gov.pl).