Warszawa,

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

DPNT.413.22.2025

Pani

Izabela Leszczyna

Minister Zdrowia

Ministerstwo Zdrowia

Szanowna Pani Minister,

działając na podstawie art. 52 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781; dalej jako: ustawa), zwracam się do Pani Minister z uprzejmą prośbą o rozważenie zasadności podjęcia prac legislacyjnych prowadzących do zmiany przepisów **rozporządzenia Ministra Zdrowia z dnia 5 sierpnia 2016 r. w sprawie szczegółowych kryteriów wyboru ofert w postępowaniu w sprawie zawarcia umów o udzielanie świadczeń opieki zdrowotnej** (Dz. U. z 2025 r. poz. 328 ze zm.)[1], **w wyniku których podmioty** ubiegające się o zawarcie umowy z Narodowym Funduszem Zdrowia (dalej jako: NFZ), o udzielanie świadczeń opieki zdrowotnej finansowanych ze środków publicznych **otrzymałyby możliwość uzyskania dodatkowych punktów w ramach procedury oceny ofert w związku z wykazaniem stosowania kodeksu postępowania, albo posiadania certyfikatu**, w rozumieniu odpowiednio art. 40 i art. 42 rozporządzenia 2016/679[2].

Przetwarzanie danych osobowych i świadczenie opieki zdrowotnej to procesy, które są ze sobą ściśle powiązane. Przetwarzanie danych osobowych musi być

[1] Wydanego na podstawie upoważnienia zawartego w art. 148 ust. 3 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2024 r. poz. 146 ze zm.).

[2] 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

zgodne z zasadami określonymi w rozporządzeniu 2016/679, a za ich realizację odpowiedzialny jest administrator, który ma obowiązek to wykazać[3]. W tym celu administrator wdraża odpowiednie środki techniczne i organizacyjne, a jeśli to niezbędne – polityki ochrony danych[4]. Stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonego mechanizmu certyfikacji może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków[5].

Art. 40 ust. 2 oraz motyw 98 rozporządzenia 2016/679 przewidują, że kodeksy postępowania mają ułatwić skuteczne stosowanie tego aktu, doprecyzowując jego zastosowanie, a także uwzględniać szczególne cechy przetwarzania danych w różnych sektorach i branżach, ze szczególnym uwzględnieniem potrzeb mikroprzedsiębiorców oraz małych i średnich przedsiębiorstw. Powołany motyw doprecyzowuje również m.in. możliwość dopasowania w tworzonych kodeksach postępowania obowiązków administratorów i podmiotów przetwarzających do ryzyka naruszenia praw lub wolności osób fizycznych na potrzeby konkretnego przypadku charakterystycznego dla danej branży bądź sektora. Z motywu zaś 77 rozporządzenia 2016/679 wynika, że kodeksy postępowania zawierać mogą wytyczne w zakresie tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie prawa przez administratora lub podmiot przetwarzający, m.in. w kontekście identyfikacji ryzyka[6].

W rozporządzeniu 2016/679 znajduje się szereg przepisów, zgodnie z którymi stosowanie przez administratorów oraz podmioty przetwarzające zatwierdzonych kodeksów postępowania ma wpływ nie tylko na ich wiarygodność, ale również może być przydatne do stwierdzenia, czy dany administrator bądź podmiot przetwarzający wywiązują się ze swoich obowiązków[7].

Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą tworzyć lub w przypadku istniejących kodeksów zmieniać je bądź rozszerzać ich zakres tak, aby doprecyzować zastosowanie RODO, uwzględniając specyfikę działalności danej branży oraz zakres przetwarzanych danych. Rozporządzenie 2016/679 nie definiuje pojęcia "zrzeszenie", a więc za dopuszczalne należy uznać przyjęcie szerokiego rozumienia tego terminu bez zawężania katalogu podmiotów uprawnionych do opracowania kodeksu postępowania pod względem struktury formalnej i organizacyjnej[8]. Jednocześnie należy zauważyć, że Europejska Rada Ochrony Danych, zrzeszająca organy ochrony danych osobowych państw członkowskich UE

[3] Art. 5 rozporządzenia 2016/679.
[4] Art. 24 ust. 1 i 2 rozporządzenia 2016/679.
[5] Art. 24 ust. 3 rozporządzenia 2016/679.
[6] *K. S. Zielińska*, Komentarz do art. 27, w: *M. Kawecki, M. Czerniawski*, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2019,, s. S. 153-154.
[7] Por. art. 24 ust. 3; art. 28 ust. 5; art. 32 ust. 3; art. 35 ust. 8; art. 46 ust. 2 lit. e rozporządzenia 2016/679.
[8] *B. Fischer*, w: *Sakowska-Baryła*, Komentarz RODO, art. 40, pkt 5, Warszawa 2018, s. 438.

wskazała, że organy tworzące kodeks postępowania muszą wykazać swą reprezentatywność dla branży, dla której kodeks powstaje[9].

Kodeksy postępowania mogą tworzyć zarówno podmioty z sektora prywatnego, jak również z sektora publicznego. Kodeksy postępowania dla sektora publicznego nie podlegają monitorowaniu przez podmioty monitorujące (art. 41 ust. 6 rozporządzenia 2016/679), ale i one muszą zawierać mechanizmy monitorowania, oparte na przepisach prawa krajowego[10].

Podkreślenia wymagają korzyści z przyjęcia kodeksów postępowania. W wytycznych 1/2019 Europejska Rada Ochrony Danych podkreśliła, już na samym wstępie (pkt 7), dobrowolność tworzenia kodeksów postępowania oraz fakt, iż mają one zawierać specyficzne rozwiązania ochrony danych osobowych dla konkretnych sektorów, branż, z zastrzeżeniem możliwości tworzenia kodeksów międzysektorowych. Kodeksy mają pomóc podmiotom z danego sektora lub też kilku sektorów (jeśli jest wspólny element, podobny zakres przetwarzania) w stosowaniu przepisów rozporządzenia 2016/679. Mają one również stanowić efektywne narzędzie pokazujące podmiotom stosującym kodeks, co jest poprawne, legalne i etyczne w działaniach konkretnego sektora. Etyka postępowania w danej branży jest rzeczą, na którą warto zwrócić uwagę. Jakkolwiek w przepisach rozporządzenia 2016/679 oraz w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych nie ma mowy wyraźnie o etyce postępowania, to jednak Wytyczne 1/2019 już w pierwszych zdaniach zwracają na to uwagę. Kodeksy postępowania, obok oceny skutków planowanych operacji przetwarzania dla ochrony danych (ang. „*Data Protection Impact Assessments*")[11] oraz certyfikacji, stanowią narzędzia, dzięki którym organizacje będą miały możliwość wykazania zgodności swych działań z rozporządzeniem 2016/679[12].

Jednocześnie kodeksy mogą stanowić skuteczne narzędzie pozwalające zyskać zaufanie osób, których dane dotyczą. Mogą one odnosić się do różnych kwestii, z których wiele może wynikać z obaw społeczeństwa lub nawet obaw odczuwanych w samym sektorze, i jako takie stanowią narzędzie służące zwiększeniu przejrzystości w stosunku do osób fizycznych w związku z przetwarzaniem ich danych osobowych[13].

Warto zauważyć, że do tej pory Prezes UODO zatwierdził dwa kodeksy postępowania – oba dla podmiotów z branży medycznej. Są nimi Kodeks postępowania dla sektora ochrony zdrowia dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających, którego wnioskodawcą była Polska Federacja Szpitali oraz Kodeks postępowania dotyczący ochrony danych

[9] Zob. Wytyczne [EROD] 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679, pp. 8 i 21 (dalej jako Wytyczne 1/2019) https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_pl .

[10] Wytyczne 1/2019, przyp. 35 i pkt 88.

[11] Należy w tym miejscu zaznaczyć, że kodeksy postępowania oraz certyfikacja stanowią dobrowolne narzędzia, podczas gdy DPIA może być obligatoryjna w określonych sytuacjach.

[12] Zob. motyw. 81 RODO.

[13] Wytyczne 1/2019 pkt 16.

osobowych przetwarzanych w małych placówkach medycznych, którego wnioskodawcą było Porozumienie Zielonogórskie. Do kodeksu wskazanego jako pierwszy (przygotowanego przez PFSz) przystępować mogą także podmioty publiczne.

Drugim dobrowolnym narzędziem określonym w rozporządzeniu 2016/679, z którego mogą korzystać administratorzy i podmioty przetwarzające, jest **certyfikacja**. Organy nadzorcze zachęcają do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z rozporządzeniem 2016/679 operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające[14]. W rozporządzeniu 2016/679 brak definicji „certyfikacji", dlatego warto posłużyć się wskazówkami EROD, zgodnie z którymi certyfikacja na podstawie art. 42 i 43 RODO dotyczy zaświadczenia osoby trzeciej odnoszącego się do operacji przetwarzania dokonywanych przez administratorów i podmioty przetwarzające[15].

Zgodnie z art. 15 ust. 1 ustawy o ochronie danych osobowych certyfikat wydawany jest 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[16].

Podobnie jak w przypadku kodeksów postępowania, w rozporządzeniu 2016/679 znajduje się szereg przepisów dotyczących certyfikacji jako mechanizmu umożliwiającego wykazywanie zgodności[17].

Analogicznie jak w przypadku kodeksów postępowania, uzyskanie certyfikatu nie wpływa na wynikający z rozporządzenia 2016/679 zakres obowiązków administratora lub podmiotu przetwarzającego, lecz jest dodatkowym formalnym narzędziem potwierdzającym dołożenie należytych starań przez organizację w aspekcie ochrony danych osobowych. Uzyskanie certyfikatu nie zwalnia więc ani z obowiązków wynikających z rozporządzenia 2016/679, ani nie zastępuje jego postanowień.

Mając na uwadze powyższe rozważania dotyczące kodeksów postępowania i certyfikacji oraz po przeanalizowaniu treści wskazanego we wstępie rozporządzenia Ministra Zdrowia z dnia 5 sierpnia 2016 r. w sprawie szczegółowych kryteriów wyboru ofert w postępowaniu w sprawie zawarcia umów o udzielanie świadczeń opieki zdrowotnej, **Prezes UODO dostrzega możliwość zwiększenia poziomu ochrony danych osobowych przy realizacji opieki zdrowotnej finansowanej ze środków publicznych oraz jednocześnie promowania kodeksów postępowania i**

[14] Motyw 100 rozporządzenia 2016/679; art. 42 ust. 1 rozporządzenia 2016/679.
[15] Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia, pkt 17.
[16] Dodatkowe wymogi akredytacji podmiotów certyfikujących (s. 5) – zatwierdzone przez Prezesa Urzędu Ochrony Danych Osobowych 8 grudnia 2023 r.
[17] Por. art. 24 ust. 3, art. 28 ust. 5, art. 32 ust. 3, art. 46 ust. 2 lit. f rozporządzenia 2016/679.

mechanizmów certyfikacji jako narzędzi umożliwiających wykazywanie zgodności z rozporządzeniem 2016/679. W ww. rozporządzeniu Ministra Zdrowia określono wykaz szczegółowych kryteriów wyboru ofert oraz warunki ich spełnienia. W świetle postanowień § 5 i 6 przedmiotowego rozporządzenia Ministra Zdrowia należy zauważyć, że członkostwo w kodeksie postępowania podlega ciągłemu monitorowaniu i w przypadku, gdy członek kodeksu nie stosuje się do jego postanowień może zostać go pozbawiony. Jednocześnie należy wskazać, że kodeks pozwala wykazać zgodność z rozporządzeniem 2016/679 jedynie w zakresie uregulowanym w tym kodeksie (postanowienia kodeksu mogą dotyczyć wybranych procesów przetwarzania danych osobowych). Podobnie w przypadku certyfikacji – jest ona udzielana administratorom lub podmiotom przetwarzającym na maksymalny okres 3 lat i może zostać przedłużona. W stosownym przypadku certyfikacja może zostać również cofnięta. Posiadanie certyfikatu świadczy o zgodności z rozporządzeniem 2016/679 jedynie w zakresie wynikającym z przedmiotu certyfikacji.

Należy też podnieść, że kodeksy postępowania tworzą pewien standard, także dla wprowadzenia odpowiednich środków bezpieczeństwa. Jest to szczególnie istotne w obszarze ochrony zdrowia, w którym dochodzi coraz częściej do cyberataków, i w którym odnotowywane są liczne naruszenia ochrony danych[18]. Punktowanie za podejmowanie dodatkowych działań zabezpieczających dane podmiotów danych to niewątpliwie będzie dobry krok dla wzmocnienia praw pacjentów i pracowników sektora medycznego.

Mając na uwadze powyższe, w ocenie Prezesa Urzędu Ochrony Danych Osobowych warte rozważenia jest wprowadzenie zmian, które umożliwiłyby przyznawanie dodatkowych punktów podczas oceny ofert w postępowaniach w sprawach zawierania umów o udzielanie świadczeń opieki zdrowotnej członkom kodeksów postępowania lub podmiotom posiadającym certyfikat w rozumieniu rozporządzenia 2016/679 – analogicznie jak przy premiowaniu posiadania certyfikatów systemów zarzadzania, o czym mowa w 6 przedmiotowego rozporządzenia Ministra Zdrowia i odpowiednich jego załącznikach. Przyznawanie punktów za przedstawienie przez świadczeniodawców takich dodatkowych gwarancji przestrzegania przepisów o ochronie danych osobowych mieści się w celach tego rozporządzenia i służyć będzie podwyższeniu standardów kontraktowania świadczeń przez NFZ.

Jeżeli przedstawiona koncepcja zyska uznanie Pani Minister, w przypadku podjęcia prac legislacyjnych przez resort zdrowia deklaruję wsparcie eksperckie Urzędu Ochrony Danych Osobowych i gotowość współpracy w celu stworzenia odpowiednich przepisów prawa. Uprzejmie proszę o odniesienie się W świetle przedstawionej powyżej argumentacji uprzejmie proszę Panią Minister o odniesienie

[18] Prezes UODO nałożył karę w wysokości 66 500 PLN na Uniwersytecki Dziecięcy Szpital Kliniczny im. L. Zamenhofa w Białymstoku za niewdrożenie odpowiednich środków technicznych i organizacyjnych. Prezes UODO nałożył też dwie kary na Centrum Medyczne Ujastek Sp. z o.o. z siedzibą w Krakowie o łącznej kwocie 1 145 891,25 zł za zamontowanie urządzeń rejestrujących obraz na 2 salach oddziału neonatologii niezgodnie z obowiązującymi przepisami oraz za niezastosowanie środków technicznych i organizacyjnych odpowiadających ryzyku dla danych przetwarzanych na kartach pamięci, które znajdowały się w urządzeniach monitorujących.

się do tego wystąpienia na piśmie **w terminie 30 dni** od daty jego otrzymania, zgodnie z dyspozycją art. 52 ust. 2 ustawy o ochronie danych osobowych.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych