Nr 1/2023 (45)
Styczeń 2023

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

Zamieszczone w „Newsletter UODO dla IOD" publikacje nie stanowią oficjalnego stanowiska UODO.

JEST NOWY WZÓR WNIOSKU O ŚWIADCZENIE RATOWNICZE DLA STRAŻAKÓW OSP

Zgodnie z zapowiedzią złożoną przez przedstawicieli MSWiA w odpowiedzi na wystąpienie Prezesa UODO (o czym informowaliśmy w Newsletterze Uodo dla IOD wyd.7/2022) znowelizowane zostało rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 lutego 2022 r. w sprawie wniosku o przyznanie świadczenia ratowniczego.

Z wzoru tego wniosku usunięto klauzulę zgody na przetwarzanie danych osobowych w zakresie niezbędnym do rozpatrzenia wniosku oraz wypłaty i obsługi świadczenia ratowniczego. Była ona kwestionowana przez organ nadzorczy jako wadliwa. Usunięto też pola na dodatkowe dane kontaktowe, takie jak numer telefonu i adres e-mail.

ROZMOWA Z EKSPERTEM

GDY TEORIA STAJE SIĘ PRAKTYKĄ

Z Moniką Krasińską, dyrektor Departamentu Orzecznictwa i Legislacji w UODO o stanie prac nad kodeksem postępowania w Polsce rozmawia Ewelina Janczylik-Foryś, UODO

W grudniu 2022 r. Prezes UODO zatwierdził „Kodeks postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych". To pierwszy w Polsce taki dokument. Co to oznacza dla pacjentów oraz dla samych placówek medycznych?

Zatwierdzony przez Prezesa UODO kodeks postępowania daje szansę na podniesienie poziomu ochrony danych osobowych przetwarzanych w związku z działalnością leczniczą realizowaną w małych placówkach medycznych, które przystąpią do kodeksu. Dla pacjentów, a także osób upoważnionych czy bliskich - bo przede wszystkim w odniesieniu do nich kodeks ma zastosowanie – oznacza on zwiększoną gwarancję, że ich dane osobowe będą przetwarzane zgodnie z zasadami określonymi zarówno w RODO, jak i w przepisach szczególnych. Ponadto może on pełnić funkcję edukacyjną, ponieważ przekazuje im wiedzę

o tym, jak powinny być przetwarzane ich dane osobowe będące w dyspozycji placówki medycznej czy lekarza, z usług których korzystają. Co ważne, informacje te są przekazywane przystępnym językiem.

Z punktu widzenia zarówno pacjentów, jaki i małych placówek medycznych kodeks ułatwia przestrzeganie praw pacjenta, ponieważ w sektorze medycznym ochrona danych osobowych wpisuje się w poszanowanie prawnie chronionych tajemnic medycznych, m.in. lekarskiej czy pielęgniarskiej.

Warto też zaznaczyć, że osoby, których dane dotyczą, skargę dotyczącą naruszenia postanowień kodeksu mogą złożyć do podmiotu monitorującego. To otwiera drogę do polubownego jej załatwienia, co przyspiesza realizację ich praw do ochrony danych.

Z kolei podmioty medyczne, które przystąpią do tego kodeksu i będą go prawidłowo stosowały, nie tylko ułatwią sobie pracę, ale zyskają pewność, że ich działania związane z przetwarzaniem danych osobowych na potrzeby działalności leczniczej są zgodne z RODO. Jednocześnie kodeks będzie dla nich skutecznym narzędziem zapewniania rozliczalności. Dla medyków ważne może okazać się także to, że kodeks po prostu ułatwi im pracę. Jego przepisy wprost bowiem wskazują, jak powinni postąpić w konkretnych sytuacjach. Jednocześnie te wskazówki i zalecenia są zgodne zarówno z RODO, jak i z przepisami szczególnymi, m.in. ustawą o prawach pacjenta, ustawą o zawodach lekarza i lekarza dentysty czy aktami wykonawczymi do nich. Ponadto uwzględniają wytyczne i opinie m.in. Europejskiej Rady Ochrony Danych (EROD).

Proszę wyjaśnić, jakie korzyści daje administratorom podejmowanie inicjatyw tworzenia kodeksów postępowania i co powinno w nich zostać uregulowane?

Kodeks postępowania – poprzez doprecyzowanie kwestii ochrony danych osobowych z uwzględnieniem specyfiki sektora czy branży, która dokonuje przetwarzania – stwarza szansę na podniesienie poziomu przestrzegania przepisów o ochronie danych osobowych. Zapewne dla wielu administratorów istotne jest też to, że stosowanie zatwierdzonego kodeksu postępowania będzie czynnikiem branym pod uwagę przez organ nadzorczy przy ocenie poszczególnych aspektów przetwarzania danych. dokonywanej w przypadku zgłoszonych naruszeń ochrony danych czy przy wydawaniu rozstrzygnięć, które będą zapadały w decyzjach administracyjnych zamykających postępowania skargowe, pokontrolne czy wszczęte z urzędu. W przypadku naruszenia przepisów RODO przestrzeganie zatwierdzonego kodeksu postępowania może mieć także wpływ na rodzaj zastosowanego środka naprawczego stosowanego przez organ nadzorczy, w tym na wysokość administracyjnej kary pieniężnej. A jeśli chodzi o to, co powinno w zostać uregulowane w kodeksie, to ważne, by znalazło się w nim rozstrzygnięcie najważniejszych problemów sektora czy branży, które go przyjmują. Nie powinien on powielać przepisów RODO. Jego celem powinna być natomiast kodyfikacja tego, jak stosować RODO w sposób konkretny, praktyczny i precyzyjny. W kodeksie nie może zabraknąć wskazania mechanizmów monitorowania i podmiotu monitorującego. Brak w tym obszarze powoduje, że takie

kodeksy nie mogą być przez nas zatwierdzone, bo tak naprawdę to jest ten element kluczowy, który służy także realizacji zasady rozliczalności.

Jak wygląda procedura zatwierdzenia kodeksu?

Od strony formalnej warunkiem przyjęcia kodeksu postępowania jest przedłożenie jego projektu organowi nadzorczemu do zatwierdzenia. Projekt taki musi spełniać wymogi określone w RODO i ustawie o ochronie danych osobowych, a także w Wytycznych EROD nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących. Przedłożenie wniosku o zatwierdzenie kodeksu postępowania wiąże się również z obowiązkiem uiszczenia opłaty skarbowej.

Co ważne, poprawnie złożony wniosek powinien zawierać informację o przeprowadzonych przed złożeniem wniosku konsultacjach publicznych oraz ich wyniku. Natomiast sama procedura zatwierdzenia kodeksu postępowania składa się z kilku etapów (patrz ramka 1).

Jednak już do samego złożenia wniosku warto dobrze się przygotować. Nieprzemyślane i nieadekwatne propozycje mogą spowalniać proces zatwierdzana kodeksu, a nawet zniechęcać do dalszej pracy nad nim. Żeby opracować kodeks trzeba mieć świadomość, że chodzi o stworzenie dojrzałych rozwiązań, akceptowanych w środowisku, które ma ten kodeks stosować. Zatem przygotowania do skonstruowania kodeksu powinna poprzedzić przede wszystkim inwentaryzacja problemów, które odnotowuje dana branża. Na tej podstawie możliwe jest wskazanie antidotum na ich rozwiązanie uwzględniające zarówno konkretne przepisy RODO, jak i mogące mieć zastosowanie przepisy krajowe. Ponadto dzięki pracom nad kodeksem administratorzy i podmioty przetwarzające mogą na nowo przyjrzeć się funkcjonującym procedurom: technicznym, organizacyjnym, a nawet tym z zakresu zarządzania organizacją. Zatem analiza tego, co ma być w kodeksie uregulowane i później poddane ocenie organu nadzorczego, powinna rozpocząć się od bardzo dokładnego przyjrzenia się, jak faktycznie funkcjonują organizacje w danej branży i jakie mają problemy. Dopiero w dalszej kolejności można przystąpić do stworzenia propozycji zapisów kodeksowych, które następnie zostaną poddane konsultacjom, o których już wspomniałam, a zwieńczeniem tego etapu będzie wniosek o zatwierdzenie kodeksu.

Jakie najczęściej błędy popełniają inicjatywy zgłaszające kodeksy postępowania?

Wiele projektów kodeksów zawiera propozycje rozwiązań, które nie są do końca przedyskutowane i przemyślane, co uniemożliwia lub utrudnia organowi nadzorczemu wszczynanie oraz prowadzenie postępowania w sprawie zatwierdzenia kodeksu.

Jeśli chodzi o przygotowanie samego kodeksu, to zauważamy wiele nieprawidłowości. Bardzo często są one związane chociażby z brakiem jasnego i zwięzłego uzasadnienia, w którym byłyby szczegółowo omówione informacje o celu kodeksu, zakresie jego stosowania, sposobie, w jaki ułatwi on skuteczne stosowanie RODO. Zdarzają się też sytuacje, w których podmiot wnioskujący o zatwierdzenie kodeksu nie reprezentuje większości sektora, a przecież twórcy kodeksu muszą wykazać, że są faktycznym organem

przedstawicielskim i rzeczywiście rozumieją potrzeby swoich członków. Innym stwierdzanym przez nas uchybieniem bywa bardzo wąski zakres konsultacji publicznych. Nie obejmują one np. osób, których dane dotyczą, użytkowników, klientów czy też organizacji, działających na ich rzecz. Bardzo często zaś przedstawiane są zbyt szczegółowe sprawozdania z konsultacji. Tymczasem rolą organu nadzorczego nie jest analiza obszernej dokumentacji, stanowiącej odzwierciedlenie całego przebiegu tego procesu. Najważniejsza jest ocena, czy konsultacje zostały przeprowadzone w odpowiednim zakresie, a także to, czy oraz jakie przepisy projektu kodeksu postępowania zostały zmodyfikowane w ich efekcie.

Inny dostrzegamy przez nas błąd, o którym już wspomniałam, to chęć uregulowania zbyt wielu kwestii. Tymczasem za tą ilością nie idzie jakość zaproponowanych rozwiązań.

Czego reprezentacje administratorów powinny unikać w czasie prac nad tworzeniem kodeksu postępowania dla swojej branży?

Proces tworzenia kodeksu jest złożony. Żeby ta praca była efektywna, wymaga wieloaspektowego podejścia (patrz ramka 2). Często w przedstawianych nam propozycjach kodeksów widoczne jest opieranie ich rozwiązań w 90% na zacytowaniu przepisów RODO. Tymczasem w kodeksie mamy pokazać, jak stosować konkretne przepisy, jakie wprowadzać rozwiązania, dlatego też wymagamy pogłębionej analizy potrzeb sektora, bo to ułatwia przyjęcia takich rozwiązań. Dobrze jeśli twórcy kodeksów będą mieli świadomość, że w tych dokumentach warto odwoływać się do przepisów sektorowych, wytycznych, opinii czy stanowisk, które zajmowane były np. przez Europejską Radę Ochrony Danych. Tylko w ten sposób pomożemy administratorom stosować kodeks, a jednocześnie realizować zasadę rozliczalności.

Kodeks opracowany przez Federację Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie to pierwsza inicjatywa, która zakończyła się wydaniem przez Prezesa UODO decyzji zatwierdzającej ten szczególny dokument. Jednak toczą się prace nad kilkoma innymi kodeksami. Jaki jest stan prac na nimi?

Dotychczas do Prezesa UODO zgłoszono jeszcze siedem formalnych wniosków o zatwierdzenie kodeksu postępowania. Wiemy, że powstało jeszcze sześć innych inicjatyw, ale dotąd nie przedłożyły one organowi nadzorczemu formalnych wniosków o zatwierdzenie projektów kodeksów. Wydaliśmy dwie pozytywnie opinie do przedłożonych nam kodeksów, m.in. opinię w sprawie zatwierdzonego już kodeksu. Ponadto przeprowadziliśmy dwa postępowania, które są związane z akredytacją. Mieliśmy również sześć wniosków o akredytację podmiotu monitorującego, z czego cztery sprawy zostały zakończone wobec nieuzupełnienia braków formalnych albo niespełnienia podstawowych kryteriów, które warunkują rozważenie udzielenia akredytacji, czyli dalsze procedowanie sprawy przez organ nadzorczy.

Polska to niejedyny kraj, w którym stosujemy RODO, i mogą powstawać kodeksy postępowania. Jaki jest stan prac nad nimi w innych krajach

Rejestr wszystkich zatwierdzonych kodeksów postępowania jest dostępny na stronie internetowej EROD. Są tam informacje zarówno o kodeksach obowiązujących w poszczególnych państwach członkowskich, jak i o kodeksach transgranicznych. Co do zasady, procedury zatwierdzania kodeksu krajowego i europejskiego (transgranicznego) są do siebie zbliżone. Niezmiernie ważne jest jednak określenie wprost w projekcie kodeksu, czy ma być on jedynie krajowy, czy dotyczyć będzie również przetwarzania danych osobowych w innych państwach członkowskich UE. Kodeks transgraniczny musi bowiem spełniać dodatkowe wymagania formalne, np. w kontekście wersji językowych. Jego projekt – odmiennie niż w przypadku kodeksów krajowych – musi zostać również zaopiniowany przez EROD. Jako organ nadzorczy jesteśmy członkiem Europejskiej Rady Ochrony Danych i uczestniczyliśmy w pracach dotyczących kodeksów postępowania, m.in. braliśmy udział w opiniowaniu dwóch kodeksów dedykowanych przetwarzaniu danych w chmurze.

Wraz z zatwierdzeniem pierwszego kodeksu postępowania, Prezes UODO wydał pierwszy certyfikat potwierdzający akredytację podmiotu monitorującego. Na czym polega rola podmiotu monitorującego przestrzeganie kodeksu postępowania?

Głównymi zadaniami podmiotu monitorującego są wspieranie merytoryczne administratorów, którzy przystąpią do kodeksu, a także nadzór nad prawidłowością przestrzegania przez nich przepisów o ochronie danych osobowych i postanowień kodeksu. Podmiot monitorujący ma prawo rozpatrywać skargi od osób, których dane są przetwarzane przez członków kodeksu. Ma także ściśle współpracować z organem nadzorczym. Stosowanie kodeksu w praktyce pozwoli zatem ograniczyć kierowanie skarg do organu nadzorczego, jak i może wpłynąć na zmniejszenie liczby zgłaszanych Prezesowi UODO naruszeń ochrony danych osobowych w danym sektorze.

Jakie warunki należy spełnić, aby zostać podmiotem monitorującym?

Za monitorowanie przestrzegania kodeksu postępowania odpowiada niezależny podmiot monitorujący, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu. Obowiązek wskazania podmiotu monitorującego nie dotyczy kodeksów odnoszących się do przetwarzania danych osobowych wyłącznie przez organy i podmioty publiczne. Nie oznacza to jednak, że taki kodeks nie musi zawierać skutecznych mechanizmów monitorowania. Muszą one być zgodne z przepisami dotyczącymi nadzoru i kontroli funkcjonującymi w danym sektorze. Organ nadzorczy dokonuje akredytacji podmiotu monitorującego dany kodeks postępowania na podstawie przepisów RODO (patrz art. 41 RODO), Wytycznych EROD nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących, ustawy o ochronie danych osobowych (patrz art. 27) oraz Wymogów akredytacji podmiotów monitorujących kodeksy. Ostatni ze wskazanych dokumentów został opracowany przez Prezesa UODO i zaopiniowany przez EROD. Można znaleźć w nim szczegółowo opisane wymogi, które musi spełnić podmiot monitorujący, aby uzyskać akredytację organu nadzorczego.

Ramka 1: Procedura zatwierdzenia kodeksu postępowania

Etap 1. Wstępna ocena projektu kodeksu

Po złożeniu do Prezesa UODO przez przedstawicieli inicjatywy kodeksowej wniosku o zatwierdzenie kodeksu postępowania wraz projektem kodeksu, organ nadzorczy bada, czy przedłożony projekt spełnia wymogi formalne oraz kryteria dopuszczalności, o których mowa w Wytycznych EROD.

Etap 2. Ocena treści przedłożonego projektu w świetle kryteriów zatwierdzania kodeksów.

Etap ten służy wyjaśnieniu treści projektu z wnioskodawcą, umożliwiając mu wprowadzenie ewentualnych modyfikacji. Kończy się on wydaniem przez organ nadzorczy opinii o zgodności przedłożonego projektu z przepisami RODO.

Etap 3. Zatwierdzenie przez Prezesa UODO kodeksu postępowania

Ostatni etap obejmuje zatwierdzenie kodeksu postępowania w formie decyzji administracyjnej, o ile organ nadzorczy uzna, że stanowi on odpowiednie zabezpieczenie właściwego stosowania RODO.

Etap 4. Rejestracja kodeksu

Zatwierdzony kodeks postępowania jest rejestrowany przez polski organ nadzorczy i EROD.

Więcej informacji na **stronie internetowej UODO w zakładce „Kodeksy postępowania"**

Ramka 2: 7 wskazówek, jak efektywnie wypracować kodeks postępowania

1. Pokaż, jak w twojej branży stosować RODO

Rozwiązania zawarte w kodeksie powinny być konkretne, a więc praktyczne i precyzyjnie opisane. Dlatego bardzo ważna jest przejrzystość zapisów, chociażby po to, żeby wyeliminować wiele ryzyk, które istnieją w często rozproszonych strukturach różnych organizacji.

2. Zapewnij jednolity standard postępowania

Zdarza się, że branże mają tożsame przepisy, ale bardzo różne procedury funkcjonowania. Mają tożsame wytyczne pochodzące np. z organów regulacyjnych, ale bardzo różne rozwiązania techniczne lub organizacyjne. Zatem te rozwiązania, które są wprowadzane w kodeksie, przede wszystkim mają wprowadzić jednolity standard, chociażby podejścia do kluczowych zagadnień, związanych z zastosowaniem RODO, np. przy tak bardzo ważnym zagadnieniu jak kształtowanie ról w procesie przetwarzania danych.

3. Wskaż czytelny podział ról i odpowiedzialności

Kodeks powinien odpowiadać na pytanie, kto jest kim w procesie przetwarzania danych, jaki jest zakres jego odpowiedzialności i jakie w związku z tym występują ryzyka. Zapisy niepełne czy nieprecyzyjne tylko będą tworzyć kolejne wątpliwości.

4. Unikaj niewłaściwej interpretacji przepisów i rozumienia obowiązków

Twórcy kodeksów powinni dążyć do eliminowania ryzyka nieadekwatnego przetwarzania danych albo wprowadzania zbędnych procesów przetwarzania danych, bo często nadmiar określonych procesów także zaburza model funkcjonowania jednostki i organizacji.

5. Zadbaj o przejrzystą komunikację
Należy upraszczać komunikację wewnętrzną w organizacjach, żeby pracownicy szybciej przekazywali sobie informacje co do zajęcia określonego stanowiska w sferze decydowania o danych osobowych czy realizacji kompetencji lub przypisanych im funkcji.

6. Pomyśl, jak zminimalizujesz ryzyka
Kodeks ma niwelować bardzo zróżnicowane szacowanie poziomu ryzyk przy tych samych stanach faktycznych, i budowania niepełnych albo w ogóle niezgodnych z przepisami rozwiązań technicznych, organizacyjnych czy bezpieczeństwa.

7. Przygotuj swoją organizację na pokonywanie trudności
Kodeks ma odpowiadać na pytanie, w jaki sposób podchodzić do ochrony danych osobowych w przypadku np. gdy dojdzie do naruszenia ochrony danych. Zatem kodeks ma z jednej strony usprawnić przyjmowanie skarg których dane dotyczą, a z drugiej strony, gdy okaże się, że skarga nie ma pokrycia w działaniach administratora, zapewnić klienta, że działania, które były wykonywane na jego danych osobowych, były prawidłowe. To pozwoli wyeliminować zgłaszanie skarg do podmiotu monitorującego i w ten sposób przyczyni się też do tego, aby ostatecznie organ nadzorczy nie musiał wyciągać konsekwencji wobec administratora.

PRZYJĘTY KODEKS UMOŻLIWI DALSZĄ POPRAWĘ STANDARDÓW OBSŁUGI PACJENTÓW

Komentarz eksperta
Bartłomiej Chmielowiec, Rzecznik Praw Pacjenta

Cieszę się, że powstał Kodeks postępowania dotyczący ochrony danych osobowych w małych podmiotach leczniczych. Jest to cenne wsparcie w realizacji obowiązku ochrony danych osobowych w placówkach medycznych i umożliwienie dalszej poprawy standardów obsługi pacjentów. Powierzenie podmiotowi wykonującemu działalność leczniczą tak szczególnej kategorii informacji łączy się ze zobowiązaniem do przetwarzania ich z poszanowaniem uprawnień pacjentów. Wymaga to zaangażowania w prowadzenie, przechowywanie i udostępnianie dokumentacji medycznej, zachowanie tajemnicy informacji związanej z pacjentem, czy dbałości o jego intymność i godność.

Stworzone wytyczne są dziś szczególnie aktualne, odpowiadają na wyzwania związane z wejściem w życie nowych regulacji, jak i pojawiających się wątpliwości dotyczących stosowania już obowiązujących norm. Wyraźnie widać to na przykładzie podmiotów wykonujących działalność leczniczą, korzystających z systemu

monitoringu wizyjnego oraz z teleporad. Możliwe niedopowiedzenia lub niezrozumienie niektórych kwestii prawnych i zasad odnoszących się do ochrony danych osobowych pacjenta w tych obszarach niejednokrotnie stanowią przedmiot naruszeń prawa pacjenta. Powstanie Kodeksu umożliwia pogłębienie wiedzy w jaki sposób należy dbać o dane osobowe w zakresie udzielania świadczeń przez podmioty wykonujące działalność leczniczą. Podnoszenie jakości udzielanych świadczeń medycznych oraz poprawa standardów bezpieczeństwa pacjentów stanowią integralną część praw pacjenta. Największe korzyści z nowych rozwiązań odnosimy zaś jeśli są one odpowiednio wdrażane. Jestem przekonany, że Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych pomoże w skuteczniejszym wdrożeniu tych zmian. Jednocześnie liczę, że będzie on również inspiracją dla przyszłych działań wszystkich uczestników systemu ochrony zdrowia.

ROZMOWA Z EKSPERTEM

BEZPIECZEŃSTWO DANYCH OSOBOWYCH PACJENTÓW JEST SZCZEGÓLNIE WAŻNE

Z Jackiem Krajewskim, prezesem Federacji Porozumienie Zielonogórskie o pierwszym przyjętym kodeksie postępowania w sektorze zdrowia rozmawia Ewelina Janczylik-Foryś, UODO

Panie Prezesie, proszę przyjąć gratulacje w związku z przyjęciem „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych", który jest nie tylko pierwszym zatwierdzonym kodeksem w sektorze ochrony zdrowia, ale pierwszym dokumentem tego typu przyjętym w Polsce. I od razu pytanie, czy było warto? Jak wyglądała współpraca z UODO nad przyjętymi postanowieniami?

Przede wszystkim chciałbym powiedzieć, że jako Federacja jesteśmy dumni z tego przedsięwzięcia, bo choć wymagało ono wiele wysiłku i pracy, to zdecydowanie było warto. Przygotowanie kodeksu wymagało ogromnego wysiłku, ale wspólnie z firmą Jamano, która doskonale rozumie specyfikę naszej branży, udało się stworzyć wyjątkowe rozwiązanie. Naszym kluczowym celem jest zapewnianie pacjentom bezpieczeństwa, które rozumiemy dużo szerzej niż tylko jako wsparcie w zakresie zdrowia, ale również całej „otoczki", która towarzyszy wizycie w gabinecie lekarskim. Takim aspektem bez wątpienia jest

bezpieczeństwo danych osobowych, które dla pacjentów jest szczególnie ważne. W obliczu wyzwań jakim są masowe cyberataki, właściwe zbieranie, przechowywanie i przekazywanie danych osobowych jest taką profilaktyką cyberprzestępczości. Jesteśmy dumni tym bardziej, że Federacja Porozumienie Zielonogórskie jako pierwsza organizacja w sektorze ochrony zdrowia stworzyła i przyjęła kodeks postępowania w zakresie RODO. Współpraca z UODO była wzorcowa, choć wymagająca, bo obydwu stronom zależało na tym, aby stworzyć dokument i wynikające z niego procedury w sposób czytelny, możliwie prosty, a jednocześnie nie pozostawiający wątpliwości i miejsca na domysły. Efekt końcowy uważam jednak za spektakularny.
Tym bardziej, że przecież przecieraliśmy szlaki – zarówno my, jak i UODO. Było to bowiem pionierskie w Polsce postępowanie administracyjne zatwierdzające kodeks postępowania.

Jakie korzyści w Pańskiej ocenie wiążą się z podjęciem inicjatywy tworzenia branżowego kodeksu postępowania?

Poczucie bezpieczeństwa u pacjentów jest bezwzględną wartością i to jest kluczowa korzyść. Kodeks pozwala na wdrożenie właściwych procedur w zakresie ochrony danych osobowych, a więc ułatwia pracę personelowi placówki, jak również minimalizuje ryzyko wycieku danych czy wątpliwości w przypadku konieczności ich przekazywania. Mówiąc krótko, daje pewien spokój, który w tak wrażliwym obszarze jak dane osobowe pacjentów jest istotny szczególnie. Projektując kodeks, mieliśmy również w zamierzeniu budowanie jednolitego standardu dla przychodni zrzeszonych w naszej Federacji. Bardzo liczę na powszechne przystępowanie małych placówek medycznych do kodeksu, dzięki czemu najlepsze praktyki w zakresie ochrony danych osobowych będą dostępne dla milionów naszych pacjentów.

Kodeks opracowany przez Porozumienie Zielonogórskie został stworzony dla tzw. małych placówek medycznych (MPM). Proszę wskazać, o jakich administratorów danych chodzi?

Chodzi tutaj o poradnie podstawowej opieki medycznej (POZ) oraz ambulatoryjnej opieki specjalistycznej (AOS), czyli placówki tzw. pierwszego kontaktu pacjenta z przedstawicielami ochrony zdrowia.
Dlatego właściwa obsługa procesu zbierania i przechowywania danych osobowych niejako na początku tej drogi pacjenta po ścieżce leczenia jest tak ważna.

Jak można przystąpić do kodeksu postępowania? W jaki sposób pacjent może upewnić się, że POZ czy gabinet lekarski jest członkiem kodeksu postępowania?

Do Kodeksu mogą przystąpić wyłącznie placówki należące do Federacji Porozumienie Zielonogórskie. Sama procedura przyjęcia Kodeksu jest natomiast bardzo prosta – wystarczy zarejestrować się na dedykowanej platformie www.kodeksrodo.pl, deklarując chęć przystąpienia. W następnym kroku akredytowany podmiot monitorujący (RS Jamano) dokonuje wstępnej kontroli danej placówki. Poradnia przystępująca do Kodeksu otrzyma następnie certyfikat potwierdzający spełnienie warunków i możliwość przyjęcia Kodeksu, co w każdym przypadku będzie umiejscowione w widocznym dla pacjentów miejscu

w przychodni. Wszystkie te kroki odbywać się będą on-line, bez zbędnych formalności, a lista placówek medycznych, które przystąpiły do kodeksu będzie publikowana na stronie RS Jamano. Zachęcam też pacjentów do wychodzenia z inicjatywą i pytania personel poradni o Kodeks, bo w końcu chodzi o wrażliwe dane chorych, a więc pacjenci mają prawo wymagać pewnych standardów w tym zakresie, szczególnie w obliczu wyzwań, o których wspomniałem wcześniej.

Co w praktyce oznacza dla pacjentów, że dana placówka medyczna, z której usług korzystają, przystąpiła do stosowania kodeksu postępowania?

Oznacza to przede wszystkim, że mogą spać spokojnie, bowiem ich dane będą pozyskiwane, przechowywane i przetwarzane zgodnie z najwyższymi standardami w tym zakresie. Dzisiaj każdy pacjent ma świadomość czym jest ochrona danych osobowych i jak ważny jest to aspekt. Pacjent ma też pewność, że jego przychodnia rodzinna robi wszystko, aby zapewnić mu bezpieczeństwo na wielu polach, nie tylko stricte medycznym, ale i tym administracyjnym. Chory ma też pewność, że pozyskane są tylko niezbędne dane osobowe, że są zbierane poprawnie, są poufne i przechowywane w sposób właściwy. Muszę tu nadmienić, że projekt Kodeksu był konsultowany z niektórymi organizacjami reprezentującymi pacjentów, dzięki czemu jesteśmy pewni, że jest on odpowiedzią na realne potrzeby chorych, jest celowanym rozwiązaniem.

KODEKS JEST ZBIOREM ZASAD, KTÓRE POMOGĄ ZAPEWNIĆ WYSOKI POZIOM BEZPIECZEŃSTWA DANYCH OSOBOWYCH PACJENTÓW

Komentarz eksperta

Paweł Makowski, RS Jamano

14 grudnia 2022 r. już zawsze będzie wyjątkową datą dla systemu ochrony danych osobowych w Polsce. Zatwierdzenie przez Prezesa UODO kodeksu postępowania otwiera dla pierwszego w Polsce sektora – tak wrażliwego przecież sektora ochrony zdrowia – możliwość stosowania najlepszych praktyk ochrony danych osobowych. Kodeksy postępowania zostały zaprojektowane, by pomóc we właściwym stosowaniu RODO poprzez wyjaśnienie i doprecyzowanie zawartych w nim postanowień. RODO nie zawiera konkretnych wskazówek, jakie środki należy wdrożyć, by chronić dane osobowe pacjentów – celem „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w placówkach medycznych”

Federacji Porozumienie Zielonogórskie jest doprecyzowanie tych przepisów i wskazanie modelowych rozwiązań. To co wyróżnia ten dokument to fakt, że został napisany jasnym i zrozumiałym językiem oraz posługuje się wieloma praktycznymi przykładami. Dzięki takiemu podejściu, placówki medyczne będą mogły znaleźć w kodeksie wyjaśnienia i wskazówki dotyczące przetwarzania danych osobowych w obszarach typowych dla sektora ochrony zdrowia, takich jak: udostępnianie dokumentacji medycznej czy też bezpieczeństwo danych w telemedycynie. Kodeks jest zatem jedynym na rynku zbiorem zatwierdzonych przez Przezesa UODO zasad, które pomogą zapewnić wysoki poziom bezpieczeństwa danych osobowych pacjentów i wykazać, że podmiot przystępujący do kodeksu zapewnia zgodność z RODO – co może także pozytywnie wpłynąć na postrzeganie placówki przez pacjentów. Aby tak się stało, Prezes UODO akredytował również podmiot monitorujący – RS Jamano – którego rolą będzie sprawdzanie, czy wszyscy członkowie kodeksu rzeczywiście stosują się do jego postanowień oraz bieżąca współpraca z Federacją na rzecz wysokich standardów ochrony danych w sektorze ochrony zdrowia. Czuję wielką satysfakcję, że mogłem ten kodeks współtworzyć i niemniejszą odpowiedzialność związaną z kierowaniem działalnością podmiotu monitorującego. Tu praca dopiero się zaczyna.

XVII DZIEŃ OCHRONY DANYCH OSOBOWYCH

Przyszłość ochrony danych osobowych w świetle rozwoju technologii" to temat ogólnopolskiej konferencji naukowej organizowanej w ramach obchodów XVII Dnia Ochrony Danych Osobowych. Urząd Ochrony Danych Osobowych organizuje to wydarzenie 31 stycznia 2023 r. we współpracy z Prezydentem Miasta Ełku oraz ełcką filią Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.

Tegoroczna konferencja odbędzie się w formule hybrydowej. Organizatorzy zaplanowali wydarzenia stacjonarne w Ełku, w siedzibie filii Uniwersytetu Warmińsko-Mazurskiego, które będą także transmitowane w Internecie za pośrednictwem strony internetowej UODO. Na program tegorocznych obchodów Dnia

Ochrony Danych Osobowych składa się konferencja naukowa oraz wydarzenia towarzyszące. Szczegółowe informacje na temat wydarzenia oraz agenda spotkania są dostępne na stronie internetowej UODO.

PROJEKT DECYZJI W SPRAWIE ADEKWATNOŚCI TRANSATLANTYCKICH RAM OCHRONY DANYCH UE-USA

Komisja Europejska 13 grudnia 2022 r. opublikowała projekt decyzji, zgodnie z którą Stany Zjednoczone zobowiązują się do zapewnienia odpowiedniego stopnia ochrony danych osobowych przekazywanych z UE do USA.

Projekt decyzji, który stanowi odpowiedź na wątpliwości Trybunału Sprawiedliwości Unii Europejskiej wyrażone w lipcu 2020 r. w sprawie Schrems II. Decyzja wskazuje na obowiązki prawne dla przedsiębiorstw i możliwości dochodzenia praw przez osoby, których dane dotyczą.

Obecnie dokument został przekazany do zaopiniowania Europejskiej Radzie Ochrony Danych (EROD). Następnie decyzja zostanie zatwierdzona przez komitet składający się z przedstawicieli państw członkowskich UE. Parlament Europejski ma również prawo kontroli decyzji dotyczących odpowiedniego stopnia ochrony. Komisja będzie mogła przyjąć ostateczną decyzję stwierdzającą odpowiedni stopień ochrony danych, po zakończeniu wszystkich wcześniejszych etapów.

Funkcjonowanie ram ochrony prywatności danych UE-USA będzie polegało na okresowym przeglądom, które będą przeprowadzane przez Komisję Europejską wraz z europejskimi organami ochrony danych oraz właściwymi organami USA. Pierwszy przegląd odbędzie się w ciągu roku od wejścia w życie decyzji stwierdzającej odpowiedni stopień ochrony danych.

Szczegółowe informacje:

Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US

Adequacy decision for the EU-US Data Privacy Framework

KARY

Portugalia: kara za niezgodne z prawem przetwarzanie danych podczas spisu powszechnego.

Portugalski organ nadzorczy nałożył administracyjną karę pieniężną na Narodowy Instytut Statystyczny w wysokości 4,3 mln euro.

Portugalczycy ustalili, że administrator naruszył różne przepisy RODO w kontekście przetwarzania danych dotyczących spisu powszechnego z 2021 r. Podczas postępowania organ nadzorczy stwierdził pięć naruszeń RODO w kontekście przetwarzania danych w ramach spisu powszechnego 2021, dotyczących następujących kwestii:

1. braku zgodności z prawem przetwarzania szczególnych kategorii danych osobowych (art. 9 ust. 1 RODO). W formularzach, które respondenci byli zobowiązani wypełnić, organ nadzorczy stwierdził, że pytania dotyczące religii i danych dotyczących zdrowia, które zgodnie z prawem miały być dobrowolne, a nie obowiązkowe, jak w przypadku pozostałych ankiet, nie zostały należycie oznaczone jako nieobowiązkowe. Brak informacji uniemożliwił respondentom kształtowanie ich wolnej woli i samostanowienie o tym, czy mają odpowiadać na pytania dotyczące szczególnych kategorii danych,

2. brak przestrzegania obowiązków w zakresie przejrzystości (art. 12 i 13 RODO), w szczególności w zakresie przekazywania jakichkolwiek informacji dotyczących operacji przetwarzania, np. poprzez wyświetlanie informacji o ochronie prywatności na stronie internetowej Instytutu lub na jakiejkolwiek innej stronie,

3. brak oceny skutków dla ochrony danych (art. 35 ust. 1, ust. 2 i ust. 3 lit. b RODO), obejmującej całość operacji przetwarzania i odpowiednie wymiary spisu. Dokument dostarczony przez administratora, jako ocena skutków dla ochrony danych, został uznany za ograniczony w zakresie i niewystarczający w stosunku do przetwarzania danych osobowych.

4. brak należytej staranności w zakresie wyboru podmiotu przetwarzającego (art. 28 ust. 1, 6 i 7 RODO), polegający na zaakceptowaniu standardowej umowy, która nie została poddana ocenie merytorycznej pod kątem wymogów art. 28 ust. 3. Administrator nie upewnił się, że podmiot przetwarzający przyjął wszystkie odpowiednie środki w celu przestrzegania zasad i przepisów RODO, w tym, że zagwarantował, że ryzyko

związane z przetwarzaniem zostało ograniczone. W ramach tej umowy przetwarzania Instytut zgodził się, że sądami właściwymi do rozstrzygania sporów będą sądy kalifornijskie.

5. brak zgodności z przepisami dotyczącymi międzynarodowego przekazywania danych (art. 44 i 46 ust. 2 RODO), zgodnie z interpretacją TSUE w wyroku w sprawie Schrems II. Administrator upoważnił podmiot przetwarzający, na podstawie umowy, do przekazywania danych do USA poprzez zawarcie standardowych klauzul umownych bez przyjęcia jakichkolwiek środków uzupełniających, a także upoważnił podmiot przetwarzający do angażowania się w działalność innych, dalszych podmiotów (pod)przetwarzających, mających swoje jednostki organizacyjne w państwach trzecich, które nie zapewniają równoważnego stopnia ochrony gwarantowanego w UE. Organ nadzorczy podkreślił również brak kontroli i wiedzy Instytutu na temat miejsca w którym znajdują się dane osobowe respondentów po ich wprowadzeniu do sieci podmiotu przetwarzającego, jak również pełną kontrolę podmiotu przetwarzającego nad narzędziami szyfrowania/ odszyfrowywania zabezpieczającymi transmisję danych.

Źródło: **decyzja organu nadzorczego**

Francja: Organ nadzorczy nałożył karę pieniężną na FREE w wysokości 300 tys. euro.

Decyzja jest następstwem postępowania, które zapoczątkowało kilka skarg dotyczących trudności napotykanych przez osoby fizyczne w uwzględnieniu ich wniosków o dostęp do danych osobowych i o ich usunięcie przez francuskiego operatora telefonicznego FREE.

Organ nadzorczy dokonał następujących ustaleń co do działań administratora:

- brak przestrzegania prawa dostępu osób. których dane dotyczą (art. 15 RODO),

- brak przestrzegania prawa osoby fizycznej do usunięcia danych (art. 12 i 21 RODO),

- niezapewnienie bezpieczeństwa przetwarzania (art. 32 RODO),

- niedopełnienie obowiązku udokumentowania naruszenia ochrony danych osobowych (art. 33 RODO).

W rezultacie francuski organ nadzorczy nałożył na FREE administracyjną karę pieniężną w wysokości 300 000 euro i postanowił podać decyzję do publicznej wiadomości. Nakazał również administratorowi uporządkowanie rozpatrywania wniosków o dostęp składanych przez osoby fizyczne oraz o wykazanie zastosowania się do nakazu w ciągu trzech miesięcy od notyfikowania decyzji, pod groźbą kary pieniężnej w wysokości 500 euro za każdy dzień zwłoki.

Źródło: **decyzja organu nadzorczego**

Pozyskiwanie nowych klientów a prawa osób, których dane dotyczą - przedsiębiorstwo EDF France ukarane karą pieniężną w wysokości 600 000 euro

Do francuskiego organu nadzorczego wpłynęły liczne skargi dotyczące trudności napotykanych przez osoby, których dane dotyczą, w realizacji ich praw przez przedsiębiorstwo EDF, które jest pierwszym przedsiębiorstwem elektrycznym we Francji.

Organ nadzorczy dokonał następujących ustaleń, co do działań administratora:

- brak pozyskiwania zgody osób fizycznych na otrzymywanie prospektów handlowych drogą elektroniczną (art. L. 34-5 francuskiego kodeksu pocztowego i komunikacji elektronicznej oraz art. 7 RODO),

- niewypełnianie obowiązków informacyjnych i brak umożliwienia wykonywania praw (art. 13 i 14 RODO),

- niezapewnienie bezpieczeństwa przetwarzania (art. 32 RODO).

Na podstawie ustalonego stanu faktycznego, francuski organ nadzorczy stwierdził, że administrator nie wywiązał się z obowiązków przewidzianych w RODO oraz we francuskim kodeksie pocztowym i komunikacji elektronicznej. Organ nałożył na EDF administracyjną karę pieniężną w wysokości 600 000 euro i podał ją do publicznej wiadomości.

Wysokość administracyjnej kary pieniężnej została ustalona z uwzględnieniem stwierdzonych naruszeń oraz współpracy ze strony przedsiębiorstwa i przy uwzględnieniu wszystkich środków, jakie podjęło ono w trakcie postępowania w celu osiągnięcia zgodności ze wszystkimi domniemanymi naruszeniami.

Szczegółowe informacje w j. francuskim dostępne na stronach:

Prospection commerciale et droits des personnes : sanction de 600 000 euros à l'encontre d'EDF
Commercial prospecting and rights of individuals: EDF fined 600 000 euros

Źródło: **edpb.europa.eu**