Nr 7/2022 (40)
Lipiec 2022

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

ZMIANY W PRZEPISACH DOTYCZĄCYCH PRZYZNAWANYCH ŚWIADCZEŃ RATOWNICZYCH

Resort spraw wewnętrznych i administracji zapowiada wszczęcie prac legislacyjnych zmierzających do wyeliminowania klauzuli zgody na przetwarzanie danych osobowych w celu rozpatrzenia wniosku oraz wypłaty i obsługi świadczenia ratowniczego przyznawanego strażakom ochotnikom.

Taką deklarację przedstawiciele MSWiA złożyli w odpowiedzi na wystąpienie Prezesa UODO. Organ nadzorczy zwrócił w nim uwagę na niedostosowanie przepisów rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 2 lutego 2022 r. w sprawie wniosku o przyznanie świadczenia ratowniczego, będącego aktem wykonawczym do ustawy z dnia 17 grudnia 2021 r. o ochotniczych strażach pożarnych, do zasad ochrony danych osobowych określonych w RODO. Wskazał, że z przepisów ww. rozporządzenia, a konkretnie ze stanowiącego załącznik do niego wniosku o przyznanie świadczenia ratowniczego, powinna zostać wyeliminowana klauzula zgody o treści: „Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie niezbędnym do rozpatrzenia wniosku oraz wypłaty i obsługi świadczenia ratowniczego”.

Zgodnie bowiem z przepisami RODO, wyrażenia zgody nie można uznawać za dobrowolną, jeżeli osoba, której dane dotycz nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.Ponadto jeżeli podstawą przetwarzania danych osobowych jest przepis prawa, nie można równocześnie traktować zgody jako przesłanki legalizującej to przetwarzanie. Dublowanie warunków przetwarzania danych określonych w art. 6 ust. 1 RODO prowadzi do naruszenia zasady przejrzystości, a także legalizmu i rzetelności.

Organ nadzorczy zaznaczył, że przepisy ustawy o ochotniczych strażach pożarnych stanowią o zasadach przyznawania świadczeń ratowniczych (art. 17 ustawy) i są wystarczające z punktu widzenia zapewnienia poszanowania zasady legalizmu i celowości. Wystąpienie przez zainteresowanego świadczeniem ze stosownym wnioskiem rodzi obowiązek przedstawienia danych osobowych zawartych w tym wniosku i obowiązek rozpatrzenia tego wniosku na zasadach przyjętych w przepisach prawa oraz dalsze przechowywanie danych w celach i terminach w nich określonych. W konsekwencji przyjmowanie rozwiązania w postaci pozyskiwania dodatkowo zgody na przetwarzanie danych w celach określonych

w odrębnych przepisach prowadzi do przyjmowania oświadczenia, które od początku obarczone jest istotną wadą wpływającą na jego skuteczność. Dodatkowo osoba, której dane dotyczą, jest wprowadzana w błąd, gdyż wycofanie zgody nie może rodzić określonych dla niej skutków prawnych i chociażby z uwagi na odrębne przepisy prawa dane nie będą usunięte wraz ze złożeniem oświadczenia o wycofaniu zgody. Przyjęcie takiego rozwiązania w praktyce prowadzi do zaistnienia swoistego konfliktu informacyjnego i niepożądane konfuzji po stronie adresatów przepisów szczegółowych, którzy mają problem z wypełnieniem przepisów ww. rozporządzenia, zwłaszcza z realizacją zasady rozliczalności.

Dodatkowo w toku prowadzonej z resortem korespondencji i przedstawianych w niej propozycji rozwiązania innych sygnalizowanych MSWiA problemów dotyczących przetwarzania danych osobowych na potrzeby przyznawania świadczeń ratowniczych organ nadzorczy wskazał, że jeśli chodzi o zawarte w analizowanym rozporządzeniu dane kontaktowe w postaci numeru telefonu oraz adresu e-mail, to należałoby je zamieścić w treści ustawy o ochotniczych strażach pożarnych, wskazując, że ich podanie jest fakultatywne, gdyż w Polsce nie istnieje obowiązek posiadania numeru telefonu oraz adresu poczty elektronicznej.

INICJATYWA OPRACOWANIA KODEKSU POSTĘPOWANIA DLA SĄDÓW

Grupa inspektorów ochrony danych z sądów rozpoczęła prace nad przygotowaniem kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w sądach.

Przedstawiciele Urzędu Ochrony Danych Osobowych 30 czerwca 2022 r. spotkali się z reprezentantami grupy inicjującej powstanie kodeksu postępowania dla sądów – inspektorami ochrony danych (IOD) z sądów apelacyjnych i okręgowych. Było ono z jednej strony okazją do przedstawienia założeń tego przedsięwzięcia, które zyskało aprobatę ze strony prezesów i dyrektorów tych sądów, których inspektorzy zaangażowani są w inicjatywę stworzenia kodeksu, a z drugiej do omówienia kwestii wymagających ze strony projektodawców szczególnej uwagi.

Inspektorzy ochrony danych wskazali, że w swojej praktyce spotykają się z niejednolitym podejściem do rozwiązywania konkretnych zagadnień związanych z ochroną danych osobowych. Problemy w ich pracy wynikają także z działania w tym obszarze wielu administratorów czy z niezależności poszczególnych jednostek.

Dlatego by rozstrzygnąć istniejące wątpliwości i stworzyć zgodny z RODO wzorzec radzenia sobie z problemami, z którymi spotykają się przy wykonywaniu swoich zadań, postanowili stworzyć kodeks postępowania.

Poinformowali, że jego zakresem zamierzają objąć jak najwięcej zagadnień, które mogą być w nim uregulowanie (tj. te, które nie wchodzą w zakres wymiaru sprawiedliwości). W związku z tym planują, by określony on został na podstawie prowadzonych w sądach rejestrów czynności przetwarzania danych osobowych.

Przedstawiciele UODO zwrócili z kolei uwagę na to, że projekt kodeksu postępowania musi być zgłoszony do zatwierdzenia organu nadzorczego przez podmioty, które można uznać za reprezentatywne dla administratorów w sądach. Ważne jest też stworzenie odpowiednich mechanizmów monitorowania przestrzegania tego dokumentu. Istotne jest również, by język kodeksu był zrozumiały nie tylko dla administratorów (członków kodeksu), ale też dla osób, których dane są przetwarzane przez sądy. Niemniej podkreślono, że ustalenie jego zawartości i formy należy do twórców kodeksu.

Osoby zainteresowane dołączeniem do tej inicjatywy lub uzyskaniem na jej temat dodatkowych informacji mogą przesłać e-mail na adres: **kodeks@ms.gov.pl**.

Jednocześnie warto przypomnieć, że pomocne w pracach nad kodeksem postępowania mogą być materiały zamieszczone na stronie internetowej UODO:

- **Jak efektywnie prowadzić prace nad kodeksem postępowania – rekomendacje UODO**
- **Najczęściej popełniane błędy przez środowiska pracujące nad projektami kodeksów postępowania**
- **Monitorowanie kodeksów. Jak stworzyć odpowiedni mechanizm? Na co zwrócić uwagę, a czego unikać**

oraz tekst opublikowany w „Newsletterze UODO dla IOD" z listopada ub.r. (nr 11/2021) pt. „Konsultacje kodeksu postępowania powinny być szerokie, lecz podsumowanie syntetyczne".

ZAWIADOMIENIA DOTYCZĄCE IOD LUB JEGO ZASTĘPCY NALEŻY PRZESYŁAĆ TYLKO W POSTACI ELEKTRONICZNEJ

Kierowane do UODO zawiadomienia dotyczące IOD lub zastępcy IOD muszą mieć postać elektroniczną. Przesłanie zgłoszenia w innej formie jest bezskuteczne.

Podmiot, który wyznaczył inspektora ochrony danych (IOD) ma obowiązek zawiadomić o tym Prezesa UODO w terminie 14 dni od dnia wyznaczenia w trybie określonym w art. 10 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Ta sama zasada dotyczy powiadomień o zmianie zgłaszanych danych oraz do powiadomienia o odwołaniu inspektora. Analogicznie należy postąpić – zgodnie z art. 11a tej ustawy – w przypadku powiadomień dotyczących zastępcy IOD.

Również zawiadomienie o wyznaczeniu IOD (zastępcy IOD) przez administratorów działających na podstawie ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości również powinno nastąpić w postaci elektronicznej zgodnie z art. 46 ust. 9 tej ustawy.

Tymczasem, mimo że przepisy w tym zakresie zobowiązani jesteśmy stosować od ponad 4 lat – wciąż zdarza się, że kierowane do UODO zawiadomienia dotyczące inspektorów ochrony danych lub zastępców inspektorów ochrony danych (związane z wyznaczeniem, odwołaniem lub zmianą danych kontaktowych IOD lub zastępcy IOD) mają nieprawidłową postać.

Dlatego po raz kolejny przypominamy, że jedynym prawidłowym i skutecznym sposobem powiadomienia jest przesłanie zawiadomienia w postaci elektronicznej opatrzonego elektronicznym podpisem kwalifikowanym albo profilem zaufanym ePUAP przez osobę lub osoby upoważnione do reprezentowania administratora. Przesłanie zgłoszenia w innej postaci, nie jest traktowane jako wywiązanie się ze wskazanych wyżej ustawowych obowiązków.

Odpowiednie elektroniczne formularze dostępne są na stronie internetowej **www.uodo.gov.pl**, w zakładce „Inspektor Ochrony Danych” (na dole strony) pod belką: Formularze zawiadomień IOD – załatw online na biznes.gov.pl. Alternatywnym sposobem zawiadomienia Prezesa UODO o danych kontaktowych inspektora ochrony danych lub zastępcy IOD oraz w przypadku niedających się rozwiązać problemów z wysłaniem zawiadomienia

przez platformę biznes.gov.pl, jest zawiadomienie, które można wysłać przez platformę **epuap.gov.pl**.

Skutecznie dostarczone do UODO (za pośrednictwem powyższych portali) zawiadomienia są potwierdzane zgłaszającemu Urzędowym Poświadczeniem Przedłożenia generowanym automatycznie przez biznes.gov.pl lub epuap.gov.pl w postaci pliku UPP.xml.

Zawiadomienia można dokonać też przez pełnomocnika. W tym celu należy dołączyć pełnomocnictwo udzielone w formie elektronicznej, opatrzone elektronicznym podpisem kwalifikowanym lub profilem zaufanym ePUAP przez osobę lub osoby udzielające pełnomocnictwa.

Więcej informacji na temat wyznaczenia i przesyłania zawiadomień dotyczących inspektora ochrony danych znaleźć można w zakładce **Inspektor Ochrony Danych** na stronie **www.uodo.gov.pl**.

Szczególnie przydatne mogą być informacje zawarte w materiałach:

- **Jak prawidłowo zawiadomić o wyznaczeniu/odwołaniu/zmianie danych IOD (zastępcy IOD)?**
- **Co zrobić w przypadku problemów technicznych związanych ze złożeniem zawiadomienia dotyczącego IOD?**

Jednocześnie warto przypomnieć, że w materiale pt. „Wielu pełnomocników błędnie, a przez to nieskutecznie, zawiadamia o wyznaczeniu IOD" zamieszczonym w „Newsletterze UODO dla IOD" z listopada ub.r. (nr 11/2021), zawarte są wskazówki związane z dokonywaniem zawiadomienia dotyczącego IOD przez pełnomocnika.

UODO ODBYŁO SPOTKANIE Z GRUPĄ ROBOCZĄ DS. OCHRONY DANYCH OSOBOWYCH PIU

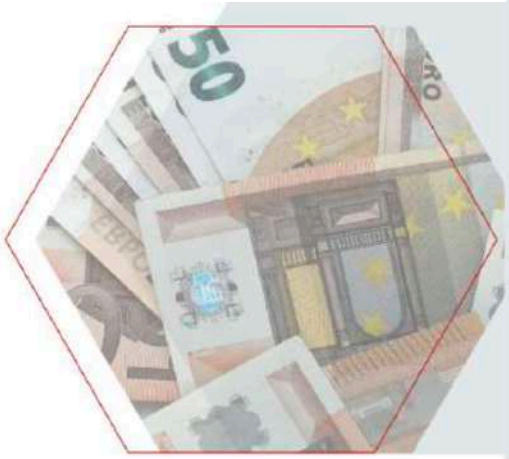
Pod koniec kwietnia br. przedstawiciele UODO odbyli spotkanie z Grupą roboczą ds. ochrony danych osobowych Polskiej Izby Ubezpieczeń. Podczas spotkania podjęto rozmowę nad opracowaniem branżowych rekomendacji opisujących organizacyjne i techniczne środki bezpieczeństwa, które mają minimalizować negatywne ryzyko naruszeń dla praw i wolności osób fizycznych.

Wskazano, iż istotne dla realizacji takiego przedsięwzięcia jest przeanalizowanie aspektów prawno-legislacyjnych tak, aby idea wypracowania standardów w zakresie ochrony danych osobowych przez ten sektor spotkała się z poparciem przedstawicieli branży, ale także była stosowana w praktyce i egzekwowana. Jak podkreślono, inicjatywa ta odbywa się na forum Grupy robaczej

PIU, która reprezentuje ok. 90% przedstawicieli sektora ubezpieczeniowego w Polsce.
UODO ze swej strony zapewniło o merytorycznym wsparciu wszystkich inicjatyw, które dążą do podnoszenia standardów bezpieczeństwa dla ochrony danych osobowych.

KARY

Włochy: sygnalizowanie naruszeń bez zachowania prywatności



Włoski organ nadzorczy nałożył administracyjną karę pieniężną na szpital publiczny i dostawcę usług IT za nieprawidłowości dotyczące systemu zgłaszania naruszeń (ang. whistleblowing).

Sprawa jest wynikiem szeregu kontroli dotyczących przetwarzania danych uzyskanych za pośrednictwem pośrednictwem systemów zarządzania informacją o zgłaszanych naruszeniach (tzw. systemów sygnalizowania naruszeń), ze szczególnym uwzględnieniem tych systemów, które są najczęściej wykorzystywane przez włoskich pracodawców.

Przedmiotowe kontrole ujawniły również naruszenia, które można było przypisać dostawcy usług informatycznych (Isweb Srl), który dostarczył ukaranemu szpitalowi publicznemu z Perugii, jako podmiotowi przetwarzającemu dane, oprogramowanie do zarządzania systemem sygnalizowania naruszeń.

System sygnalizowania naruszeń śledził dostęp do oprogramowania, ponieważ połączenia z aplikacją do sygnalizowania naruszeń były rejestrowane i przechowywane dziennikach zapory sieciowej, dzięki czemu można było śledzić użytkowników aplikacji, w tym potencjalnych sygnalistów. Pracownikom nie przekazano żadnych informacji na temat przetwarzania danych osobowych do celów zgłaszania naruszeń.

Dodatkowo ustalono, że: nie przeprowadzono oceny skutków dla ochrony danych; w rejestrze czynności przetwarzania danych osobowych nie znaleziono wpisu dotyczącego tej czynności przetwarzania; dane uwierzytelniające, które umożliwiały kierownikowi ds. korupcji i przejrzystości dostęp do systemu do zgłaszania naruszeń, zostały niewłaściwie wykorzystane podczas zmiany na kolejną osobę.

Stwierdzono również konkretne naruszenia dotyczące dostawcy usług informatycznych, który jako podmiot przetwarzający dane dostarczył szpitalowi aplikację do sygnalizowania naruszeń. Dostawca usług informatycznych nie uregulował swoich relacji z dostawcą usług hostingowych zarówno wtedy, gdy działał jako podmiot przetwarzający (na rzecz szpitala), jak i wtedy, gdy działał jako odrębny administrator (w odniesieniu do swoich usług wewnętrznych, np. w zakresie zarządzania pracownikami lub czynności księgowych i administracyjnych).

Administrator nie ustanowił odpowiednich środków technicznych i organizacyjnych w celu zapewnienia odpowiedniego stopnia bezpieczeństwa, uwzględniając szczególne ryzyko wynikające z przedmiotowego przetwarzania, co wymagało wdrożenia systemu zarządzania informowaniem o naruszeniach zgodnego z zasadami uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych – również w świetle opinii wydanej w tym zakresie przez inspektora ochrony danych szpitala (IOD).

Dostawca usługi do sygnalizowania naruszeń nie uregulował swoich stosunków z dostawcą usług hostingowych, na którym się opierał, zarówno w odniesieniu do wielorakich czynności przetwarzania, w których był administratorem (z naruszeniem art. 28 ust. 1 i 3 RODO) – począwszy od zarządzania swoimi pracownikami, poprzez czynności księgowe i administracyjne, aż po przetwarzanie nieodłącznie związane ze świadczeniem swoich usług – jak i w odniesieniu do czynności przetwarzania, w których był podmiotem przetwarzającym działającym w imieniu swoich klientów, w tym szpitala publicznego w Perugii (z naruszeniem art. 28 ust. 2 i 4 RODO).

Zarówno na szpital publiczny, jak i na dostawcę usług informatycznych nałożono administracyjną karę pieniężną w wysokości 40 tys. euro.

Źródło: **decyzja włoskiego organu**

Węgry: kwestie ochrony danych w związku z wykorzystaniem sztucznej inteligencji

Węgierski organ nadzorczy stwierdził w jednej z firm świadczących usługę telefonicznej obsługi klienta poważne naruszenie licznych artykułów RODO przez długi okres, nakazał administratorowi zaprzestanie przetwarzania informacji dotyczących stanu emocjonalnego klientów, kontynuowanie przetwarzania danych jedynie w przypadku zapewnienia zgodności z RODO oraz nałożył administracyjną karę pieniężną w wysokości około 650 tys. euro.

Administrator rejestruje wszystkie rozmowy telefoniczne dotyczące obsługi klienta. Każdej nocy oprogramowanie automatycznie analizuje wszystkie nowe nagrania audio. Oprogramowanie wykorzystuje sztuczną inteligencję do wyszukiwania słów kluczowych i odgaduje stan emocjonalny klienta w momencie rozmowy. Wynik analizy jest przechowywany w systemie oprogramowania przez 45 dni wraz z rozmową

telefoniczną. Wynikiem analizy jest lista osób przyporządkowanych wg prawdopodobieństwa niezadowolenia, na podstawie rozgniewania klienta, nagranego podczas audio rozmowy telefonicznej z działem obsługi klienta. Na podstawie wyników analizy wyznaczeni pracownicy oznaczają klientów, do których ma zadzwonić dział obsługi klienta, próbując ocenić powody ich niezadowolenia. Osoby, których dane dotyczą, nie otrzymały żadnych informacji o tym konkretnym przetwarzaniu danych i nie mają technicznej możliwości wniesienia sprzeciwu, a przetwarzanie danych zostało zaplanowane i przeprowadzone ze świadomością tego faktu.

Ocena skutków dla ochrony danych przeprowadzona przez administratora potwierdziła również, że w analizowanym przetwarzaniu danych wykorzystuje się sztuczną inteligencję, co powoduje poważne ryzyko dla podstawowych praw i wolności osób, których dane dotyczą. Ani w ocenie skutków, ani w ocenie uzasadnionego interesu nie przedstawiono żadnych faktycznych środków ograniczających ryzyko, a środki przewidziane jedynie na papierze (informacje, prawo do sprzeciwu) były niewystarczające i nieistniejące. Sztuczna inteligencja jest w swojej istocie trudna do wdrożenia w sposób przejrzysty i bezpieczny, dlatego konieczne są dodatkowe zabezpieczenia. Ze względu na jej wewnętrzne działanie, trudno jest potwierdzić wyniki przetwarzania danych osobowych przez sztuczną inteligencję, może być ona stronnicza.

Źródło: **decyzja organu nadzorczego**

Islandia: kara pieniężna m.in. za niezgodne z prawem wykorzystanie adresu e-mail

Do islandzkiego organu nadzorczego wpłynęła skarga dotycząca wykorzystania adresu e-mail skarżącego w HEI ehf., medycznym biurze podróży w Islandii, a także sposobu rozpatrzenia przez spółkę wniosku skarżącego o dostęp do danych.

W swojej decyzji islandzki organ nadzorczy zauważył, że pracownik HEI ehf. uzyskał adresy e-mail skarżącego i kilku innych lekarzy, logując się na wewnętrznej stronie Islandzkiego Stowarzyszenia Medycznego, do której dostęp miał lekarz będący członkiem rodziny pracownika. HEI wykorzystała listę mailingową do wysłania ukierunkowanej wiadomości e-mail do lekarzy, w tym do skarżącego. Ustalając wysokość administracyjnej kary pieniężnej, islandzki organ nadzorczy uznał, że mimo iż HEI uznała się za upoważnioną do korzystania z listy, nic w tej sprawie nie dowodziło, że spółka upewniła się co do zgodności z prawem przetwarzania danych.

Co więcej, wniosek skarżącego o dostęp nie został rozpatrzony zgodnie z prawem. Po tym, jak skarżący zażądał dostępu do swoich danych, spółka usunęła jego dane. Dlatego też spółka nie mogła odpowiedzieć na pytania islandzkiego organu nadzorczego dotyczące liczby lekarzy znajdujących się na liście mailingowej.

Źródło: **decyzja organu nadzorczego (https://edpb.europa.eu/news/national-news/2022/icelandic-sa-hei-medical-travel-agency-fined-unlawful-use-e-mail-address_en**