Nr 4/2022 (37)
Kwiecień 2022

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

OCENA PRZESTRZEGANIA PRZEPISÓW DOTYCZĄCYCH FUNKCJONOWANIA IOD

RODO nakłada na administratora bardzo konkretne obowiązki dotyczące zapewnienia IOD warunków do prawidłowego funkcjonowania i wykonywania przez inspektora zadań. Obecnie – w związku z rozpoczętą przez Urząd akcją weryfikacji przestrzegania obowiązujących w tym zakresie przepisów – wezwane podmioty będą musiały wykazać się podjętymi w tym celu działaniami, przedstawiając odpowiednie dowody na ich poparcie.

Organ nadzorczy od lat wskazuje, że inspektorzy ochrony danych (IOD), dysponujący odpowiednią wiedzą i umiejętnościami, a także mający odpowiednią pozycję w organizacji, w której funkcjonują, stanowią fundament skutecznego systemu ochrony danych osobowych. Dla administratora realizują bowiem istotne funkcje: weryfikacyjną i doradczą. Jednocześnie pełnią inną ważną rolę – punktu kontaktowego, czyli pośrednika między administratorem lub podmiotem przetwarzającym a osobami, których dane dotyczą, oraz między administratorem lub podmiotem przetwarzającym a organem nadzorczym.

Żeby zapewnić IOD właściwe funkcjonowanie, w RODO wprowadzono odpowiednie, mające to gwarantować przepisy. Za ich przestrzeganie i odpowiednie wdrożenie odpowiada administrator. To na niego (na kierownictwo podmiotu będącego administratorem) RODO nakłada bardzo konkretne obowiązki dotyczące nie tylko wyznaczania inspektora ochrony danych, posiadania przez niego właściwych kwalifikacji i gwarancji niezależności, ale też zapewnienia, aby wyznaczony inspektor mógł prawidłowo realizować swoje zadania. W tym kontekście ważne jest wykonanie starannych analiz, wypracowanie odpowiednich mechanizmów oraz skutecznych, poddawanych stałym przeglądom procedur działania.

Organ nadzorczy od dawna z uwagą podchodził do realizacji przez administratorów ich obowiązków dotyczących funkcjonowania IOD (a wcześniej ABI). Identyfikował występujące w tym obszarze trudności i wątpliwości oraz udzielał co do nich wskazówek i wyjaśnień, m.in. publikując na stronie internetowej UODO w zakładce Inspektor Ochrony Danych odpowiedzi na pytania, jakie przedstawiali w tym zakresie inspektorzy oraz administratorzy. Zamieszczane wskazówki miały na celu ułatwienie im wywiązywania się z nałożonych przepisami RODO obowiązków i zadań oraz wypracowanie odpowiednich, dostosowanych do ich organizacji rozwiązań. Poza tym UODO weryfikował stosowanie przepisów RODO w toku czynności kontrolnych, wzywał do składania wyjaśnień, reagując w ten m.in. sposób na wpływające do Urzędu sygnały dotyczące nieprawidłowości w tym zakresie.

W ostatnim czasie zaś, bazując na tych doświadczeniach, przygotował zestaw szczegółowych pytań, mających na celu wieloaspektową weryfikację przestrzegania przepisów dotyczących tej funkcji. Ich lista została przedstawiona w komunikacie „Weryfikacja przestrzegania przepisów dotyczących inspektora ochrony danych" zamieszczonym na stronie internetowej UODO.

Po niemalże 4-letnim już okresie stosowania RODO, każdy administrator powinien umieć wykazać się szczegółowymi, dostosowanymi do swojej działalności

rozwiązaniami w zakresie poszczególnych obowiązków wynikających z przepisów o ochronie danych osobowych dotyczących inspektorów ochrony danych. Jednocześnie warto przypomnieć, że na stronie internetowej UODO oraz w „Newsletter UODO dla IOD" sukcesywnie zamieszczane były wyjaśnienia i stanowiska odnoszące się do wielu kwestii związanych z wyznaczeniem inspektora, jego właściwym funkcjonowaniem oraz prawidłowym wykonywaniem przez niego zadań.

Poniżej prezentujemy ich zestawienie:

Wyznaczanie IOD

- Kto może, a kto musi wyznaczyć IOD na podstawie RODO?

- Wyznaczenie IOD na podstawie ustawy wdrażającej dyrektywę policyjną (DODO)

- Wyznaczenie IOD w sądach powszechnych

- W jaki sposób należy oceniać kwalifikacje osoby kandydującej do pełnienia funkcji IOD?

- Czy IOD powinien być wyznaczany na podstawie takich samych kwalifikacji jak było w przypadku ABI?

- Czy IOD musi odbyć szkolenie dla IOD oraz posiadać certyfikat potwierdzający jego odbycie?

- Czy można powołać więcej niż jednego IOD?

- Czy IOD może być pracownikiem administratora?

- Czy z zewnętrznym IOD należy zawrzeć umowę powierzenia?

- Czy z zewnętrznym IOD wykonującym zadania dla banku należy zawrzeć umowę powierzenia?

- Czy funkcję IOD może pełnić osoba spoza organizacji administratora/podmiotu przetwarzającego?

- Czy istnieje możliwość wyznaczenia osoby prawnej do sprawowania funkcji IOD?

- Czy funkcję IOD może pełnić obcokrajowiec?

- Ile maksymalnie podmiotów będzie mógł obsługiwać jeden IOD?

- Czy różni przedsiębiorcy niewchodzący w skład tej samej grupy mogą powołać jednego IOD?

- Czy po wejściu stosowania RODO CUW może powołać jednego IOD dla wszystkich obsługiwanych jednostek?

- Czy podmioty publiczne mogą powołać jednego IOD poza sytuacją uregulowaną w art. 37 ust. 3 RODO?

- Wyznaczenie IOD w straży gminnej (miejskiej) umiejscowionej w strukturze urzędu

- Czy należy wyznaczyć IOD w niepublicznym zakładzie opieki zdrowotnej mając około 2 000 pacjentów?

- Czy kierownik urzędu stanu cywilnego jest administratorem i czy musi wyznaczyć IOD?

Zapewnienie kontaktu z IOD

- Czy dane kontaktowe IOD muszą być łatwo dostępne?

- Czy administrator musi podać imię i nazwisko IOD na stronie internetowej?

- Rola IOD jako punktu kontaktowego dla osób, których dane dotyczą

Gwarancje niezależności i zapewnienie prawidłowego funkcjonowania IOD

- Jakie gwarancje niezależności zostały przyznane IOD w przepisach RODO?

- IOD nie może podlegać sekretarzowi miasta

- Administrator nie może przerzucać swoich obowiązków na IOD

- Czy praca IOD może być kontrolowana?

- Czy IOD może być osoba pełniąca funkcję kierownika komórki w organizacji?

- Przewodniczący związków zawodowych nie może być IOD

- Czy członek zarządu stowarzyszenia może być w nim jednocześnie inspektorem ochrony danych?

- Czy osoba spokrewniona z osobą zarządzającą może być IOD?

- Czy możliwe jest łączenie funkcji IOD z obowiązkami administratora systemu informatycznego (ASI)?

- Czy funkcję IOD można łączyć z wykonywaniem zawodu adwokata lub radcy prawnego?

- Czy IOD może jednocześnie pełnić funkcję pełnomocnika do spraw ochrony informacji niejawnych?

- Czy można łączyć funkcję IOD z zadaniami związanymi z obsługą wniosków od sygnalistów?

- Czy administrator jest zobowiązany na podstawie RODO do zapewnienia inspektorowi zespołu IOD?

- Czy obowiązek z art. 38 ust. 2 RODO dotyczy administratora korzystającego z usług zewnętrznego IOD?

- Czy zastępca IOD powinien być wyznaczony na stałe?

- IOD może mieć dwóch zastępców

Zadania IOD

- Jakie zadania ma IOD?

- Na czym polega wykonywanie zadań przez IOD z należytym uwzględnieniem ryzyka?

- W jaki sposób identyfikować osoby, które zwracają się do IOD jako punktu kontaktowego?

- Czy IOD jest zobowiązany wykonywać swoje zadania również na rzecz zakładowej organizacji związkowej?

- Czy prowadzenie rejestru czynności powinno być zaliczane do zadań IOD?

- Czy IOD może w imieniu administratora zawierać umowy powierzenia?

- Czy IOD powinien sporządzić plan audytów?

Odrębnym zagadnieniem jest prawidłowe zawiadamianie Prezesa UODO o wyznaczeniu IOD lub jego zastępcy, a także przesyłanie innych zawiadomień dotyczących IOD, do czego zobowiązują przepisy prawa. Kwestie te są szczegółowo omówione na stronie internetowej UODO w zakładce Zawiadomienia Prezesa UODO związane z IOD.

JAK INFORMOWAĆ O WYNIKACH NABORU NA STUDIA WYŻSZE I DO SZKÓŁ DOKTORSKICH

Wskazanie przez ustawodawcę, że wyniki postępowania w sprawie przyjęcia na studia wyższe i do szkół doktorskich są jawne nie oznacza szerokiego i niekontrolowanego publikowania danych osobowych uczestników tych postępowań rekrutacyjnych np. w Internecie.

Zgodnie z przepisami ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce wyniki postępowania w sprawie przyjęcia na studia są jawne (art. 72 ust. 5). Podobna regulacja obowiązuje w odniesieniu do rekrutacji do szkoły doktorskiej następującej w drodze konkursu, którego wyniki są jawne (art. 200 ust. 6).

Jawność nie oznacza powszechnej dostępności

Podkreślić jednak należy, że pojęcie „jawności wyników postępowania rekrutacyjnego" nie powinno być rozumiane jako równoznaczne z pojęciem „powszechnej dostępności". Samo postępowanie rekrutacyjne nie jest jawne, a dostęp do związanych z nim danych mają jego strony, ewentualnie inne podmioty uprawnione na podstawie przepisów prawa. Jawność wyników postępowania powinna być rozumiana jako możliwość zapewnienia dostępu do danych osobowych – w określonym zakresie, czasie i miejscu – w sposób umożliwiający dokonanie oceny procesu rekrutacji przez zainteresowanych jej przebiegiem uczestników postępowania rekrutacyjnego (tzw. jawność wewnętrzna).

Z przepisów powołanej regulacji nie wynika obowiązek udostępniania wyników rekrutacji w sposób zapewniający rozpowszechnienie ich na rzecz nieograniczonej grupy potencjalnych odbiorców, np. na stronie internetowej szkoły lub w BIP. W przypadku takiego upublicznienia danych osobowych, mają oni – bez spełnienia dodatkowych warunków – możliwość łatwego ich pozyskiwania i dalszego wykorzystywania w różnych celach, bez zapewnienia kontroli dotychczasowego administratora.

Zapewnienie poszanowania RODO

Zarówno uczelnia, jak i podmiot prowadzący szkołę doktorską muszą pamiętać, że jako administratorzy danych osobowych kandydatów na studia/do szkoły doktorskiej są odpowiedzialni za przetwarzanie ich zgodnie ze standardami określonymi w RODO, w tym zasadami adekwatności i minimalizacji.

Muszą też m.in. określić okresy retencji danych, pamiętając m.in. o zasadzie ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO) i zasadzie celowości (art. 5 ust. 1 lit. b RODO).
Okres ujawniania danych dotyczących wyników postępowania rekrutacyjnego powinien zaś być uzależniony przede wszystkim od celów, dla jakich dane osobowe zostały zebrane, a następnie ujawnione, zaś po ich osiągnięciu dane osobowe powinny zostać usunięte.

Warto rozważyć doprecyzowanie przepisów

Z wpływających do UODO sygnałów wynika, że obecne ukształtowanie przepisów stwarza stosującym je podmiotom pewne trudności, a ich lakoniczność powoduje, że w praktyce kształtowane są różne standardy ochrony danych osobowych uczestników postępowań rekrutacyjnych na studia i do szkół doktorskich.

UODO uznał, że uzasadniony jest postulat stworzenia przepisów, które kompleksowo, w jasny i precyzyjny sposób regulować będą kwestie jawności postępowania przy ogłaszaniu wyników naboru na uczelnie i do szkół doktorskich. Dlatego wniosek o rozważenie przygotowania takich regulacji skierował do Ministra Edukacji i Nauki. W odpowiedzi resort wskazał, że dotychczas do MEiN (wcześniej MNiSW) nie wpływały sygnały o przypadkach nieprawidłowości w dostępie do danych o wynikach rekrutacji na studia/do szkoły doktorskiej. Jednocześnie zapewnił, że ze względu na wagę omawianego zagadnienia, kwestie przedstawione w wystąpieniu Prezesa UODO zostaną rozważone w czasie prac nad ewentualną kompleksową nowelizacją ustawy – Prawo o szkolnictwie wyższym i nauce.

SPOSÓB SPRAWDZANIA NIEKARALNOŚCI OSOBY UBIEGAJĄCEJ SIĘ O ZATRUDNIENIE LUB ZATRUDNIONEJ W BANKU

Podmiot sektora finansowego, chcąc sprawdzić niekaralność osoby, którą zamierza przyjąć do pracy lub już zatrudnia, ma prawo żądać jedynie złożenia przez nią stosownego oświadczenia. Ma też prawo żądać udokumentowania przedstawionych informacji, ale może ono nastąpić wyłącznie przez przedłożenie stosownej informacji z Krajowego Rejestru Karnego, wydawanej osobie, której dane dotyczą.

Pracodawca, na mocy przepisów ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym, jest w określonych sytuacjach uprawniony do pozyskiwania informacji o osobach, których dane osobowe zgromadzone zostały w tym rejestrze. Jak bowiem stanowi art. 6 ust. 1 pkt 10 tej ustawy, prawo do uzyskania informacji o osobach, których dane osobowe zgromadzone zostały w rejestrze, przysługuje pracodawcom, w zakresie niezbędnym dla zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej.

Jednak gdy pracodawcą jest podmiot sektora finansowego wskazany w przepisach ustawy z dnia 12 kwietnia 2018 r. o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych w podmiotach sektora finansowego, a więc np. bank, to wówczas zastosowanie znajdują przede wszystkim przepisy tej ustawy. Wyraźnie wskazują one, w jakich sytuacjach, w jakiej formie i w jakim terminie następuje udzielenie podmiotowi sektora finansowego informacji o niekaralności oraz jej udokumentowanie.

Stosownie do art. 3 ust. 1 tej ustawy, podmiot sektora finansowego ma prawo żądać od osoby ubiegającej się o zatrudnienie na terytorium Rzeczypospolitej

Polskiej na stanowisku związanym z zarządzaniem mieniem tego podmiotu lub osób trzecich, dostępem do informacji prawnie chronionych, podejmowaniem decyzji obarczonych wysokim ryzykiem utraty mienia tego podmiotu lub osób trzecich lub wyrządzenia innej znacznej szkody temu podmiotowi lub osobom trzecim, a także, z zastrzeżeniem ust. 2 pkt 2, od osoby zatrudnionej na terytorium Rzeczypospolitej Polskiej na takim stanowisku udzielenia informacji dotyczących skazania prawomocnym wyrokiem za przestępstwa, o których mowa w wymienionym przepisie – a osoba ubiegająca się o zatrudnienie lub osoba zatrudniona obowiązana jest do udzielenia takich informacji na żądanie podmiotu sektora finansowego.

Udzielenie podmiotowi sektora finansowego informacji dotyczących skazania prawomocnym wyrokiem za przestępstwo następuje w formie oświadczenia osoby, której informacje te dotyczą (art. 4 ust. 1). Podmiot sektora finansowego ma prawo żądać udokumentowania udzielonych informacji, z tym że udokumentowanie takie może nastąpić wyłącznie przez przedłożenie temu podmiotowi informacji z Krajowego Rejestru Karnego, wydanej na podstawie art. 7 ust. 1 ustawy o Krajowym Rejestrze Karnym, który przewiduje, że każdemu przysługuje prawo do uzyskania informacji, czy jego dane osobowe zgromadzone są w rejestrze. Informacja taka nie może być wydana wcześniej niż 3 miesiące przed dniem jej przedłożenia temu podmiotowi (art. 4 ust. 2).

Możliwe jest także przedłożenie przez osobę ubiegającą się o zatrudnienie lub osobę zatrudnioną kopii informacji z KRK, pod warunkiem przedstawienia do wglądu również oryginału takiej informacji (art. 4 ust. 3).

Osoba występująca z zapytaniem o udzielenie informacji z Krajowego Rejestru Karnego w związku z żądaniem udokumentowania udzielonych informacji, wskazuje we wniosku zakres danych, które mają być przedmiotem informacji, odpowiadający zakresowi określonemu w art. 3 ust. 1 (art. 4 ust. 5).

KARY

Włochy: kara 20 mln euro za użycie systemu rozpoznawania twarzy

Włoski organ nadzorczy nałożył karę pieniężną w wysokości 20 mln euro na spółkę Clearview AI Inc. Zakazał jej dalszego gromadzenia i przetwarzania danych oraz usunięcie danych, w tym danych biometrycznych, przetwarzanych przez system rozpoznawania twarzy w odniesieniu do osób przebywających na terytorium Włoch. Ponadto nakazał wyznaczenie przedstawiciela na terytorium UE.

Włoski organ nadzorczy wszczął postępowanie z urzędu w następstwie doniesień prasowych oraz skarg dotyczących kilku kwestii związanych z produktami do rozpoznawania twarzy, które były oferowane przez amerykańską spółkę Clearview.

Z ustaleń włoskiego organu wynika, że dane osobowe będące w posiadaniu firmy, w tym dane biometryczne i geolokalizacyjne, były przetwarzane niezgodnie z prawem bez odpowiedniej podstawy prawnej. Zdaniem włoskiego organu nie można uznać

uzasadnionego interesu firmy z siedzibą w USA jako podstawy prawnej przetwarzania.

Ustalono także, że firma naruszyła kilka podstawowych zasad RODO, takich jak przejrzystość, ograniczenie celu i ograniczenie przechowywania. Ponadto administrator ten nie wywiązał się z obowiązku przekazania informacji, które należy podać w przypadku zbierania danych osobowych od osoby, której dane dotyczą (art. 13 RODO). Dodatkowo nie przekazywał informacji, które należy podać, jeżeli dane osobowe nie zostały uzyskane od osoby, której dane dotyczą (art. 14 RODO). Nie informował również w odpowiednim terminie o działaniach podjętych na wniosek dotyczący realizacji prawa dostępu osoby, której dane dotyczą (art. 15). Spółka nie wyznaczyła przedstawiciela w UE.

Źródło: decyzja włoskiego organu

Szwecja: region Uppsala z karą 1,9 mln koron szwedzkich za naruszenia bezpieczeństwa

Szwedzki organ nadzorczy w swoich dwóch decyzjach stwierdził, że region Uppsala nie zastosował wystarczających środków technicznych i organizacyjnych, aby zapewnić odpowiedni poziom bezpieczeństwa w stosunku do ryzyka związanego z przetwarzaniem danych osobowych. Przetwarzanie tych danych w obu przypadkach odbywało się z naruszeniem własnych wytycznych regionu.

Szwedzki Organ Ochrony Danych (IMY) otrzymał dwa zawiadomienia o naruszeniach ochrony danych osobowych od regionu Uppsala. Naruszenia dotyczyły informacji należących do szczególnej kategorii przesłanych bez szyfrowania do odbiorców w Szwecji i poza jej granicami.

Jedno z prowadzonych postępowań dotyczyło danych osobowych szczególnej kategorii i numerów ubezpieczenia społecznego przesyłanych pocztą elektroniczną z danymi pacjentów, które zostały wysłane automatycznie do odpowiednich organów służby zdrowia w regionie. Część wiadomości e-mail z danymi pacjentów, została wysłana ręcznie do naukowców i lekarzy w regionie.

Z kolei drugie postępowanie dotyczyło sposobu wysyłania przez Szpital Uniwersytecki w Uppsali wiadomości e-mail z danymi pacjentów do krajów trzecich, czyli spoza UE.

Źródło: decyzja organu szwedzkiego

Irlandia: 17 mln euro za naruszenia ochrony danych przez Meta

Irlandzka Komisja Ochrony Danych nałożyła na Meta Platforms Ireland Limited (dawniej: Facebook Ireland Limited) karę pieniężną w wysokości 17 mln euro za naruszenie zasady rozliczalność w zakresie zasad ochrony danych oraz za brak wdrożenia odpowiednich środków technicznych i organizacyjnych.

Decyzja była następstwem postępowania w sprawie transgranicznej, wszczętej w 2018 roku, w sprawie serii powiadomień o naruszeniu ochrony danych.

Ponieważ rozpatrywana przez irlandzki organ nadzoru sprawa dotyczyła przetwarzania „transgranicznego", podlegała procesowi wspólnego podejmowania decyzji (art. 60 RODO). Wszystkie pozostałe europejskie organy nadzorcze zostały zaangażowane jako współdecydujący.

Źródło: Oświadczenie prasowe Komisji Ochrony Danych

Finlandia: klinika medyczna ukarana, bo uniemożliwiała skorzystanie z prawa dostępu do danych

Fiński organ nadzorczy nałożył administracyjną karę pieniężną w wysokości 5 tys. euro za brak możliwości skorzystania z prawa dostępu do danych. Ponadto udzielono spółce upomnienia za naruszenie ogólnego rozporządzenia o ochronie danych oraz nakazano dostosowanie procedur do RODO.

Klient kliniki medycznej złożył skargę do Biura Rzecznika Ochrony Danych Osobowych, ponieważ nie otrzymał od tej placówki medycznej swojej dokumentacji pacjenta. Fiński organ nadzorczy zwrócił się do administratora danych – do kliniki medycznej – o informację, jednak ta nie złożyła stosownego oświadczenia w tej sprawie.

Zdaniem fińskiego organu klinika nie umożliwiła klientowi skorzystania z prawa dostępu do własnych danych zgodnie z RODO oraz nie podała powodu ograniczenia tego prawa. Klinika nie poinformowała również w odpowiedni sposób swoich klientów o przetwarzaniu danych osobowych, ani o tym, w jakim zakresie pełniła rolę administratora danych w odniesieniu do dokumentacji pacjentów prowadzonej w ramach jej działalności.

Zdaniem organu praktyki stosowane przez przedsiębiorstwo były systematyczne, a ponadto naruszenie było długotrwałe i dotyczyło dużej liczby osób, których dane dotyczą. Dlatego zdecydowano o nałożeniu na klinikę administracyjnej kary pieniężnej w wysokości 5 tys. euro. Ponadto fiński organ nadzorczy udzielił spółce upomnienia za naruszenie RODO i nakazał jej zmianę procedury w celu dostosowania się do przepisów o ochronie danych osobowych w zakresie informowania osób, których dane dotyczą oraz realizacji ich praw.

Źródło: decyzja fińskiego organu

RADA EUROPY

Rumunia 17. państwem, które ratyfikowało Konwencję 108+

Od 9 marca 2022 r. Rumunia należy do grona państw, które ratyfikowało zmodernizowaną konwencję nr 108 (konwencja nr 108+).

Rumunia jest stroną konwencji nr 108 od 1 czerwca 2002 r. Wejście w życie Konwencji 108+ ma zasadnicze znaczenie w erze cyfrowej. Do wejścia w życie tej fundamentalnej Konwencji, która jest przełomowym instrumentem mającym na celu zapewnienie odpowiedniej ochrony, jakiej poszukuje jednostka w coraz bardziej rozwijającej się erze cyfrowej, w celu zachowania godności i intymnej sfery prywatnej oraz pełnego korzystania z prawa do samostanowienia informacyjnego, potrzeba jeszcze wielu ratyfikacji.

WARTO WIEDZIEĆ

UODO poszukuje kandydatów do pracy

Urząd Ochrony Danych Osobowych poszukuje kandydatów do pracy od specjalisty do głównego specjalisty. Obecnie rekrutacja jest prowadzona w Departamencie Współpracy Międzynarodowej i Edukacji, Departamencie Skarg oraz w Departamencie Komunikacji Społecznej.

Zachęcamy do bieżącego śledzenia ofert pracy UODO!

Szczegółowe informacje o prowadzonych rekrutacjach są dostępne na stronie internetowej UODO w zakładce Praca.

EROD poszukuje ekspertów w ramach nowej grupy wspierającej

Europejska Rada Ochrony Danych (EROD) poszukuje ekspertów z całego Europejskiego Obszaru Gospodarczego (EOG) do współpracy z organami nadzorczymi. Chodzi o współpracę na różnych etapach działań organów związanych z prowadzeniem postępowań i egzekwowaniem prawa w dziedzinie ochrony danych.

EROD dąży do utworzenia grupy ekspertów wspierających, w której znajdą się wykwalifikowani eksperci w takich dziedzinach, jak: audyt IT, bezpieczeństwo stron internetowych, mobilne systemy operacyjne i aplikacje, Internet Rzeczy, chmura obliczeniowa, reklama behawioralna, techniki anonimizacji, kryptologia, sztuczna inteligencja, projektowanie UX, FinTech, data science, prawo cyfrowe itp.

Grupa ekspertów wspierających EROD jest kluczową inicjatywą strategiczną Rady, która pomaga organom nadzorczym w zwiększaniu ich zdolności do nadzorowania i egzekwowania ochrony danych osobowych.

Ogłoszenie EROD w j. angielskim
Szczegóły procesu rekrutacyjnego dostępne są na stronie EROD
Instrukcja przesyłania aplikacji w j. angielskim

WARTO PRZECZYTAĆ

Wytyczne francuskiego organu nadzorczego dotyczące roli IOD

Nowe wytyczne francuskiego organu ochrony danych (CNIL) wskazują na ważne aspekty, które należy wziąć pod uwagę przy powoływaniu wewnętrznego lub zewnętrznego inspektora ochrony danych (IOD).

Większość wytycznych odnosi się do powoływania IOD w dowolnym kraju Europejskiego Obszaru Gospodarczego.

Wytyczne odnoszą się również do niezależności i zasobów IOD.

Wytyczne CNIL dla Inspektorów Ochrony Danych w języku angielskim

Źródło: informacja o wydaniu wytycznych

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

Znajdująca się na naszej stronie internetowej zakładka „Inspektor Ochrony Danych" została wzbogacona o kolejne zagadnienia.

Wyjaśnienia dotyczą takich kwestii, jak:

Czy prawo dostępu do danych osobowych można realizować przez pełnomocnika?

Czy szkoła może udostępnić CUW kopię rejestru czynności przetwarzania?

W jakim języku należy wypełnić obowiązek informacyjny?

URZĄD OCHRONY DANYCH OSOBOWYCH