



## Europejska Rada Ochrony Danych przyjęła nowe wytyczne

Podczas posiedzenia plenarnego, które odbyło się 4 czerwca 2019 r. Europejska Rada Ochrony Danych (EROD) przyjęła ostateczną wersję wytycznych w sprawie kodeksów postępowania, załącznika do wytycznych w sprawie akredytacji podmiotów certyfikujących oraz załącznika do wytycznych w sprawie certyfikacji. Dokumenty te zostały przyjęte po przeprowadzeniu konsultacji publicznych.

### Wytyczne dotyczące kodeksów postępowania

Celem wytycznych jest zapewnienie praktycznych wskazówek i pomocy w interpretacji stosowania art. 40 i 41 RODO. Mają one pomóc w wyjaśnieniu procedur i przepisów dotyczących przedkładania, zatwierdzania i publikacji kodeksów postępowania zarówno na szczeblu krajowym, jak i europejskim. Wytyczne te powinny ponadto stanowić jasne ramy dla wszystkich właściwych organów nadzorczych, EROD i Komisji, umożliwiające spójną ocenę kodeksów postępowania oraz usprawnienie procedur związanych z procesem oceny.

[treść wytycznych wraz z załącznikami \(en\)](#)

### Załącznik do wytycznych w sprawie akredytacji podmiotów certyfikujących

Celem załącznika do wytycznych w sprawie akredytacji podmiotów certyfikujących jest udostępnienie wskazówek dotyczących

interpretowania i wykonywania przepisów art. 43 RODO. Przede wszystkim mają one pomóc państwom członkowskim, organom nadzorczym i krajowym jednostkom akredytującym w ustanowieniu spójnej i ujednoliconej podstawy na potrzeby akredytowania podmiotów certyfikujących. W załączniku zawarto wytyczne dotyczące dodatkowych wymogów w zakresie akredytowania podmiotów certyfikujących, które powinny zostać wprowadzone przez organy nadzorcze. Te dodatkowe wytyczne, przed ich przyjęciem przez organy nadzorcze, powinny zostać przedłożone Europejskiej Radzie Ochrony Danych do zatwierdzenia zgodnie z art. 64 ust. 1 lit. c RODO.

[treść wytycznych wraz z załącznikiem \(en\)](#)

### Załącznik do wytycznych w sprawie certyfikacji

Głównym celem przyjętego załącznika do wytycznych w sprawie certyfikacji jest określenie nadrzędnych kryteriów, które mogą mieć zastosowanie do wszystkich typów mechanizmów certyfikacji wydanych zgodnie z art. 42 i 43 RODO. W załączniku zidentyfikowano główne zagadnienia, które organy nadzorcze ds. ochrony danych oraz EROD wezmą pod uwagę i zastosują podczas zatwierdzania kryteriów certyfikacji dla mechanizmu certyfikacji.

[treść wytycznych wraz z załącznikami \(en\)](#)

### Tematy numeru

1. EROD przyjęła nowe wytyczne
2. Ułatwianie realizacji praw jest obowiązkiem administratorów
3. Rozporządzenie w sprawie zadań IOD na gruncie ustawy z 14 grudnia 2018 r.
4. Podanie numeru PESEL w decyzji administracyjnej nie ma podstawy prawnej
5. Udostępnianie danych straży miejskiej przez operatorów telekomunikacyjnych
6. Informacje o toczących się postępowaniach karnych kandydata do pracy
7. Przetwarzanie danych w związku z ZFŚS
8. Przetwarzanie danych poręczycieli przez urząd pracy
9. Komendant straży gminnej jako niezależny administrator
10. Nowe pytania w zakładce dla IOD
11. Podsumowanie IX edycji programu „Twoje dane - Twoja sprawa”
12. UODO w mediach



**Szkolenia UODO dla inspektorów ochrony danych**



**Transmisje z wydarzeń organizowanych przez UODO**

## Ułatwienie osobom fizycznym wykonywania ich praw określonych w RODO jest obowiązkiem wynikającym wprost z przepisów prawa

W wielu skargach kierowanych do Prezesa UODO osoby fizyczne wskazują na istotne kłopoty w odnalezieniu kontaktu do administratora oraz skierowaniu do niego żądania związanego z wykonywaniem praw określonych w art. 15 – 22 RODO. Sugerują, że niektórzy administratorzy celowo utrudniają swoim klientom lub interesantom identyfikację administratora i kontakt z nim, po to aby uniknąć wysiłku związanego z respektowaniem uprawnień osób, których dane przetwarzają. Kierowane do nas skargi najczęściej wskazują, że część administratorów nie przestrzega obowiązku zapewnienia osobom fizycznym przejrzystego i sprawnie działającego kanału komunikacji służącego realizacji praw tych osób.



– i gdy ma to zastosowanie bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Administrator powinien zapewnić możliwość wnoszenia odnośnych żądań także drogą elektroniczną,

z prawem, rzetelności i przejrzystości wynikającej z art. 5 ust. 1 lit. a RODO. Umożliwienie łatwego i szybkiego kontaktu z administratorem czy wyznaczonym przez niego inspektorem ochrony danych oraz właściwe spełnienie obowiązku informacyjnego ma kluczowe znaczenie dla przestrzegania powyższej zasady. Rzetelne i przejrzyste przetwarzanie oznacza, że osoba, której dane dotyczą, jest informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać jej wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Informacje przekazywane osobie muszą być między innymi łatwo dostępne i zrozumiałe, formułowane jasnym i prostym językiem (motyw 58 i 60 RODO).

W interesie administratorów i wspierających ich inspektorów ochrony danych jest zatem dbanie o to, aby osoby, których dane dotyczą nie miały problemów z dotarciem do informacji o przetwarzaniu ich danych i możliwościach realizowania swoich uprawnień określonych w RODO.

### Najczęściej sygnalizowane problemy to:

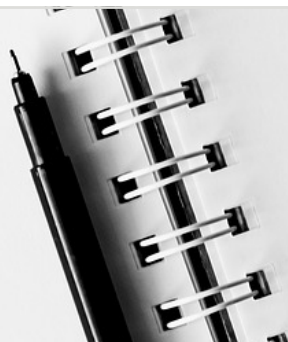
- 1) brak wskazania jakichkolwiek form kontaktu w sprawach związanych z przetwarzaniem danych osobowych;
- 2) nieudostępnianie danych dotyczących administratora i inspektora ochrony danych lub ukrywanie ich na trudno dostępnych podstronach lub w trudnych do zlokalizowania dokumentach takich jak polityka bezpieczeństwa czy regulamin świadczenia usług;
- 3) udostępnianie nieaktualnych danych kontaktowych lub nieaktualnego lub nieaktywnego formularza jako jedynej drogi kontaktu;
- 4) brak wyjaśnienia klientom, kto ponosi odpowiedzialność za działalność prowadzoną pod określoną nazwą sklepu, punktu usługowego lub portalu internetowego i do kogo powinni oni kierować swoje pytania

- 5) niewyznaczenie w ramach struktury organizacyjnej osoby odpowiedzialnej za obsługę lub przekierowanie żądań osób, których dane dotyczą, do właściwej komórki lub braku przepływu informacji w organizacji o takich żądaniach;
- 6) brak właściwej komunikacji między administratorem a podmiotem przetwarzającym w zakresie przekazywania żądań przedkładanych przez osobę, której dane dotyczą;
- 7) nieprzestrzeganie określonych w przepisach RODO terminów rozpatrywania żądań osób, których dane dotyczą.

Tymczasem ułatwienie osobie, której dane dotyczą, wykonania jej praw jest obowiązkiem wynikającym wprost z art. 12 ust. 2 RODO. W motywie 59 RODO wyjaśniono, że należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia, w tym mechanizmy żądania

w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną. Jest zobowiązany udzielić odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki – najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania – podać tego przyczyny. Wymienione praktyki administratorów stoją też w sprzeczności z zasadą zgodności

Osoby rzetelnie i uczciwie poinformowane o przetwarzaniu ich danych, mające poczucie, że ich dane nie są wykorzystywane bez ich wiedzy i kontroli, w dużo mniejszym stopniu skłonne są do występowania z żądaniami do administratorów lub składania skarg do Prezesa UODO.





## Od 6 czerwca br. obowiązuje rozporządzenie w sprawie trybu i sposobu realizacji zadań przez inspektorów ochrony danych w podmiotach objętych ustawą z dnia 14 grudnia 2018 r.

Z dniem 6 czerwca 2019 r. zaczęło obowiązywać rozporządzenie Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych (Dz.U.2019.1041). Rozporządzenie wydane

zostało w oparciu o upoważnienie określone w art. 47 ust. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

## Podanie numeru PESEL w decyzji administracyjnej nie ma podstawy prawnej

Prezes UODO stoi na stanowisku, że do oznaczania stron postępowania nie powinno się wykorzystywać numeru PESEL. Pogląd ten został potwierdzony wyrokiem WSA w Warszawie, który odrzucił skargę na jedną z decyzji Prezesa UODO.

Decyzja Prezesa UODO dotyczyła działania powiatowego inspektora nadzoru budowlanego (PINB), który wykorzystał numer PESEL dla oznaczenia stron postępowania administracyjnego dotyczącego legalności dobudowy. Jednocześnie zamieścił go w decyzji administracyjnej przesłanej siedmiu stronom tego postępowania.

Osoby, których dane w ten sposób upubliczniono, wniosły na takie postępowanie PINB skargę do Prezesa UODO, inicjując tym samym rozpoczęcie postępowania w tej sprawie.

Powiatowy inspektor nadzoru budowlanego, składając wyjaśnienia przed organem ds. ochrony danych osobowych wskazał, że działał zgodnie z art. 107 § 1 Kpa (decyzja zawiera m.in. oznaczenie strony lub stron postępowania) oraz z art. 27 § 1 pkt 2 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (tytuł wykonawczy zawiera wskazanie imienia i nazwiska lub firmy zobowiązanego i jego adresu, a także NIP lub numeru PESEL, jeżeli zobowiązany taki numer posiada).

W wydanej w tej sprawie decyzji Prezes UODO uznał, że działanie PINB było nieprawidłowe. Zazaczył, że z art. 107 § 1 Kpa nie wynika, aby elementem



obligatoryjnym oznaczenia strony było podanie numeru PESEL. W postępowaniu administracyjnym danymi identyfikującymi osobę fizyczną są bowiem: imię, nazwisko oraz adres. Inne dane mogą być podawane tylko wówczas, gdy wynika to wprost z przepisu prawa.

Prezes UODO podkreślił jednocześnie, że zamieszczenie numerów PESEL w decyzji administracyjnej jest niezgodne z zasadą minimalizacji określoną w art. 5 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych (RODO).

Jak wskazał, dopiero niewykonanie zobowiązania wynikającego z decyzji administracyjnej rozpoczęłoby bieg nowej procedury, prowadzonej zgodnie z przepisami o postępowaniu egzekucyjnym w administracji. I to na tym etapie legalne byłoby przetwarzanie numeru PESEL, który – zgodnie z art. 27 § 1 pkt 2 ustawy o postępowaniu egzekucyjnym w administracji musi być zamieszczony w wystawionym tytule wykonawczym.

Ponieważ jednak analizowana sytuacja miała charakter nieodwracalny, Prezes UODO mimo stwierdzonego naruszenia – nie mógł

Rozporządzenie dotyczy między innymi prowadzenia przez inspektorów ochrony danych sprawdzeń na skutek wystąpienia Prezesa UODO. Zgodnie z § 5 tego rozporządzenia, realizacja zadania inspektora ochrony danych określonego w art. 47 ust. 1 pkt 3 ustawy (tj. monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych z przepisami niniejszej ustawy oraz innymi przepisami dotyczącymi ochrony danych) może nastąpić także w ramach prowadzonych sprawdzeń, o których mowa w art. 11 ust. 1 tej ustawy. O przeprowadzenie takiego sprawdzenia, Prezes UODO może zwrócić się bezpośrednio do inspektora ochrony danych wyznaczonego przez administratora podlegającego ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

nakazać usunięcia numerów PESEL z decyzji PINB. Organ ds. ochrony danych osobowych nie ma bowiem uprawnień do ingerowania w treść decyzji wydawanych przez inne organy. Dlatego zmuszony był odmówić uwzględnienia wniosku skarżących. Do PINB wystąpił jednak z wnioskiem o podjęcie działań mających na celu wyeliminowanie takiej niewłaściwej praktyki w przyszłości. Skarżący – niezadowoleni z takiego rozstrzygnięcia – wnieśli skargę na decyzję Prezesa UODO do Wojewódzkiego Sądu Administracyjnego w Warszawie. Sąd jednak skargę oddalił (wyrok z dnia 20 marca 2019 r., sygn. akt II SA/Wa 2211/18).

Decyzja Prezesa UODO

Orzeczenie WSA w Warszawie

Komunikat UODO z 31 października 2018 r.



## **Straż miejska ma prawo zwrócić się do operatora telekomunikacyjnego o udostępnienie niezbędnych jej danych osobowych**

Straż miejska ma prawo zwrócić się do operatora telekomunikacyjnego o udostępnienie niezbędnych jej danych osobowych – tak wynika z wyroku Naczelnego Sądu Administracyjnego z dnia 14 marca 2019 r. (sygn. akt I OSK 1429/17). Wyrok NSA został wydany w wyniku złożonej skargi kasacyjnej od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie

z dnia 31 stycznia 2017 r. (sygn. akt II SA/Wa 1431/16) w sprawie ze skargi na decyzję Generalnego Inspektora Ochrony Danych Osobowych w przedmiocie przetwarzania danych osobowych. Tym samym NSA podzielił stanowisko zawarte w decyzji ówczesnego GIODO.

W uzasadnieniu NSA wskazał, że uzyskanie przez straż miejską

podstawowych danych osobowych abonenta telefonu komórkowego, których jedynym dysponentem był operator telekomunikacyjny, w celu ustalenia sprawcy wykroczenia, stanowiło niezbędny warunek realizacji ustawowych zadań tego podmiotu, określonych w przepisach ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych, realizowanych dla dobra publicznego. Jak przypomniano, zgodnie z art. 10a pkt 1 ustawy o strażach gminnych, straż w celu realizacji zadań ustawowych może przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane te dotyczą, uzyskane w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia. Orzeczenie jest prawomocne.

Orzeczenie NSA



## **Pracodawca nie ma prawa żądać od kandydata do pracy informacji o toczących się wobec niego postępowaniach karnych**

W odpowiedzi na jedno ze skierowanych do niego pytań Prezes UODO stwierdził, że pracodawca nie może żądać od kandydata do pracy informacji o toczących się i niezakończonych postępowaniach karnych. Zgodnie z art. 22<sup>1</sup> Kodeksu Pracy – katalog danych, które mogą być przetwarzane przez pracodawcę jest zamknięty, co oznacza, że pracodawca nie może przetwarzać danych, które wykraczają poza ten zakres. Pracodawca jest również podmiotem uprawnionym do pozyskiwania informacji z Krajowego Rejestru Karnego 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.

Pracodawca nie może żądać od osoby ubiegającej się o zatrudnienie informacji o toczących się postępowaniach karnych oraz o ich przebiegu, gdyż nie mieszczą się one w katalogu danych, które mogą

być przez niego przetwarzane. Toczące się postępowanie karne nie musi bowiem doprowadzić do prawomocnego skazania danej osoby. Informacji o toczących się postępowaniach karnych nie zawiera również Krajowy Rejestr Karny, w którym wskazuje się dane, m.in. o osobach prawomocnie skazanych oraz przeciwko którym prawomocnie umorzono postępowanie karne.

## Zasady przetwarzania danych osobowych członków rodziny pracownika w związku z korzystaniem ze świadczeń ZFŚS

Nowy art. 8 ust. 1a, dodany do ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych, nie wpływa na zmianę stanowiska Urzędu Ochrony Danych Osobowych dotyczącego zasad przetwarzania danych osobowych na potrzeby korzystania z usług i świadczeń finansowanych z zakładowego funduszu świadczeń socjalnych.

Zgodnie z przepisami tej ustawy, zarówno przyznawanie świadczeń, jak i ich wysokość uzależnione są od spełnienia przez osobę ubiegającą się o dane świadczenie określonych kryteriów socjalnych. Zgodnie natomiast z art. 8 ust. 1 ww. ustawy pracodawca ma obowiązek uzależnić udzielenie ulgi lub świadczenia od sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej do korzystania z Funduszu.

Przy ustalaniu wysokości świadczenia znaczenie ma sytuacja życiowa i materialna wszystkich członków rodziny pracownika, z którymi prowadzi on wspólne gospodarstwo domowe. Jeżeli zatem przyznawanie świadczeń jest uzależnione od

kryterium socjalnego, to oznacza, że sytuacja pracownika lub innej osoby uprawnionej do korzystania z funduszu wymaga każdorazowo jej określenia, czyli przetwarzania danych osobowych pracownika i członków jego rodziny. Przetwarzanie tych danych nie może jednak prowadzić do gromadzenia ich w zakresie szerszym, niż jest to konieczne dla realizacji celu, w jakim dane są pozyskiwane. Dodany do ustawy o zakładowym funduszu świadczeń socjalnych art. 8 ust. 1a określa, że pracownik przekazuje te dane pracodawcy w formie oświadczenia. Natomiast potwierdzenie danych w nim zawartych może odbywać się, m.in. na podstawie oświadczeń i zaświadczeń o sytuacji życiowej (w tym zdrowotnej). Należy również wskazać, że przepisy ustawy o zakładowym funduszu świadczeń socjalnych nigdzie nie wskazują, aby członkowie rodzin pracowników musieli podpisywać dodatkowe oświadczenia. Z regulacji tych wynika, że oświadczenie na temat jego sytuacji rodzinnej (w tym zdrowotnej) przedstawia pracownik.

W opinii UODO, jeżeli na potrzeby

udokumentowania spełnienia określonych kryteriów pracodawcy przydatny byłby dostęp do różnych dokumentów, np. PIT-u małżonka, to powołana regulacja umożliwia jemu jedynie wgląd do nich, ale nie daje prawa do przechowywania ich kopii. Powodowałoby to bowiem gromadzenie danych w szerszym zakresie, niż jest to niezbędne do celu przetwarzania. W dokumencie takim jak, np. PIT współmałżonka znajdują się również takie dane, jak np. nazwa zakładu pracy, czy numer PESEL, które nie są niezbędne do potwierdzenia danych przedstawionych w oświadczeniu pracownika.

Zatem, mając na uwadze, że jedną z głównych zasad dotyczących przetwarzania danych osobowych wynikających z RODO jest zasada minimalizacji danych, należy pamiętać, aby przetwarzane dane były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora (w tym przypadku pracodawcy).



## Powiatowe urzędy pracy mogą nadal przetwarzać dane o dochodach i zobowiązaniach finansowych poręczycieli

W związku z nowelizacją przepisów ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy, które zaczęły obowiązywać od 4 maja 2019 r., został uchylony art. 46 ust. 5a tej ustawy, który wskazywał, jakie dane osobowe osób występujących w charakterze poręczycieli miał prawo przetwarzać starosta. Działający w jego imieniu powiatowy urząd pracy, oprócz danych typowo identyfikacyjnych, miał prawo przetwarzać również dane

dotyczące sytuacji majątkowej poręczycieli, takie jak: uzyskiwane dochody z podaniem ich źródła i kwoty oraz aktualne zobowiązania finansowe, z podaniem wysokości miesięcznej spłaty zadłużenia.

Wobec wątpliwości urzędów pracy co do przetwarzania danych o dochodach i zobowiązaniach finansowych poręczycieli, UODO wskazał, że obecnie podstawę legalizującą przetwarzanie przez powiatowy urząd pracy danych osobowych poręczycieli

stanowią łącznie przepisy art. 33 ust. 5a i 5b ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz § 10 ust. 3 rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 14 lipca 2017 r. w sprawie dokonywania z Funduszu Pracy refundacji kosztów wyposażenia lub doposażenia stanowiska pracy oraz przyznawania środków na podjęcie działalności gospodarczej.

Przepisy ustawy o promocji zatrudnienia dają podstawę do przetwarzania danych osobowych poręczycieli, tj.: imienia i nazwiska; numeru PESEL, a w przypadku jego braku - rodzaju, serii i numeru dokumentu potwierdzającego tożsamość; adresu zameldowania na pobyt stały lub czasowy oraz adresu do korespondencji. Natomiast przepisy ww. rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej dookreślają ten katalog danych osobowych. W przypadku poręczenia refundacji, poręczyciel przedkłada staroście oświadczenie o uzyskiwanych dochodach ze wskazaniem źródła i kwoty dochodu oraz o aktualnych zobowiązaniach finansowych z określeniem wysokości miesięcznej spłaty zadłużenia, podając jednocześnie imię, nazwisko, adres zamieszkania, numer PESEL, jeżeli został nadany, oraz nazwę i numer dokumentu potwierdzającego tożsamość.

## Komendant straży w strukturach gminy jako niezależny administrator



Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. z 2018 r. poz. 928, ze zm.) w art. 10a ust. 2 wprost określiła, że komendanci straży gminnej i miejskiej są administratorami danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Przy czym - z perspektywy tej ustawy i określonych w niej obowiązków - nie ma znaczenia fakt, czy komendanci straży znajdują się w strukturze urzędu gminy, czy funkcjonują w ramach samodzielnych jednostek.

Są zobowiązani do zadbania, aby wymogi określone w powyższych przepisach zostały spełnione, a zatem między innymi w zakresie:

- realizacji praw osób, których dane dotyczą,
- opracowania i wdrożenia polityki ochrony danych osobowych,
- zgłaszania naruszeń ochrony danych osobowych Prezesowi UODO
- wyznaczenia inspektora ochrony danych

[więcej na temat wyznaczenia IOD](#)

## Wyszukiwarka decyzji Prezesa UODO

Zachęcamy do stałego śledzenia zakładki PRAWO/DECYZJE PREZESA UODO, wzbogacanej na bieżąco o kolejne anonimizowane decyzje. Przegląd decyzji ułatwią Państwu udostępnione przez nas filtry umożliwiające wyszukiwanie rozstrzygnięć według zagadnień, których one dotyczą, lub daty wydania decyzji.

[czytaj więcej](#)



## Nowe pytania w zakładce IOD na naszej stronie internetowej

Funkcjonująca na naszej stronie zakładka „Inspektor Ochrony Danych” w sekcji „Wyznaczenie i status IOD” została wzbogacona o kolejne zagadnienia. Nowe pytania i odpowiedzi dotyczą następujących kwestii:

[Czy istnieje możliwość wyznaczenia osoby prawnej do sprawowania funkcji IOD?](#)

[Czy funkcję IOD można łączyć z wykonywaniem zawodu adwokata lub radcy prawnego, a jeżeli tak to jakie warunki muszą być spełnione?](#)

Zachęcamy do stałego śledzenia naszej zakładki!

## Rekordowa liczba placówek oświatowych uczestniczyła w IX edycji programu UODO dla szkół „Twoje dane – Twoja sprawa”

Seminarium podsumowujące IX edycję ogólnopolskiego programu edukacyjnego „Twoje dane - Twoja sprawa” odbyło się w Warszawie w dniu 11 czerwca 2019 r. Wzięło w nim udział około 2000 nauczycieli oraz ponad 45000 uczniów z 335 placówek edukacyjnych z całego kraju. W tym roku szkolnym w ramach programu aż 4000 lekcji poświęcono ochronie danych osobowych

i prywatności. Podczas seminarium była okazja do rozmowy z przedstawicielami UODO w kwestiach związanych z ochroną danych osobowych. Najczęściej poruszane tematy dotyczyły umów powierzenia, kiedy i jak spełniać obowiązek informacyjny, legalności udostępniania danych.

[czytaj więcej](#)

## DZIAŁANIA UODO W MEDIACH

**876 publikacji na temat działań Urzędu Ochrony Danych Osobowych ukazało się w czerwcu 2019 roku w mediach. Szczególną aktywność przejawiały w tym zakresie media internetowe (809 informacji), jednak nie brakowało także zainteresowania ze strony mediów tradycyjnych, przede wszystkim prasy (67).**

Wiele uwagi dziennikarze poświęcili stanowiskom Urzędu w kilku ważnych dla opinii publicznej sprawach. Były to: stanowisko dotyczące działania PZU w związku z ofertą darmowego ubezpieczenia dzieci w zamian za wyrażenie zgód na przetwarzanie ich danych, a także wystąpienie do

Ministra Cyfryzacji o dostosowanie aktualnych regulacji prawnych dotyczących kwalifikowanego podpisu elektronicznego do zasad wyrażonych w RODO. Prezes UODO wypowiedział się także w kwestii, czy ostaną nowelizacja Kodeksu pracy dała pracodawcom uprawnienia do badań alkometrem.

Media chętnie prezentowały także wskazówki UODO na temat ochrony danych osobowych podczas wakacji, które Urząd przygotował w związku z rozpoczęciem sezonu urlopowego. Dziennikarze odnotowali także inne inicjatywy UODO, np. podsumowanie IX edycji programu edukacyjnego dla szkół „Twoje dane – Twoja sprawa”, w tym informowali o wynikach konkursów, które odbyły się w ramach tego programu. Sporo uwagi poświęcili również doświadczeniom UODO z pierwszego roku

stosowania RODO, m.in. w jednostkach samorządu terytorialnego, na co miała wpływ sejmowa konferencja poświęcona temu tematowi i udział w niej ekspertów Urzędu.

Do najaktywniejszych mediów, które często informowały w minionym miesiącu o działalności UODO, wśród prasy tradycyjnej należały dzienniki, np. Dziennik Gazeta Prawna oraz Rzeczpospolita. Także specjalistyczne czasopisma, jak Gazeta Ubezpieczeniowa, Gazeta Podatkowa oraz Głos Nauczycielski.

Z kolei wśród mediów internetowych o wspomnianych działaniach UODO informowały zarówno media lokalne, np. [gdynia.pl](#) czy [gospodarkapodkarpacka.pl](#), jak i te o zasięgu ogólnopolskim – [rp.pl](#) czy [prawo.pl](#).