



Krajowe organy nadzorcze, Prezes UODO i procedura one stop shop

W niniejszym artykule zajmiemy się tematyką krajowych organów nadzorczych, pozycją Prezesa Urzędu Ochrony Danych i procedury one stop shop, która w dobie ogólnoeuropejskich korporacji ma niebagatelne znaczenie.

Większość osób zajmujących się praktyką w zakresie ochrony danych osobowych, potrafi wskazać czym jest organ nadzorczy, natomiast zapewne nie wszyscy wiedzą jakie dokładnie są kompetencje tych organów.

W uzupełnieniu tego zagadnienia przyjrzymy się jakie prawa i obowiązki oraz pozycję w ustawodawstwie krajowym, pełni Prezes Urzędu Ochrony Danych Osobowych. Na zakończenie omówimy czym jest organ wiodący, jak ustalić, który to organ, jakie ma prawa i czemu służy procedura one stop shop.

Krajowe organy nadzorcze

Definicja organu nadzorczego znajduje się w art. 51 ust. 1 RODO. Jest to co najmniej **jeden niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz w celu ułatwiania swobodnego przepływu danych osobowych.**

Każde z państw członkowskich jest zobligowane do powołania **co najmniej jednego** takiego organu, zapewniając mu niezależność oraz określając sposób jego funkcjonowania. Państwa członkowskie są zobligowane do informowania o przyjętych regulacjach, a także przekazywania informacji o jakichkolwiek zmianach w funkcjonowaniu organu nadzorczego.

Kolejnym wymogiem jest **niezależność** zarówno samego organu jak i poszczególnych jego członków, którzy mają być wolni od jakichkolwiek wpływów pośrednich i bezpośrednich, a także nie mogą otrzymywać jakichkolwiek instrukcji. Treść art. 52 RODO potwierdza zapis motywu 120 – przepis ten zapewnia by organ nadzorczy posiadał zasoby kadrowe, techniczne i finansowe oraz infrastrukturę i pomieszczenia niezbędne do skutecznego wypełniania swoich zadań i uprawnień, w tym w zakresie wzajemnej pomocy, współpracy i uczestnictwa w pracach Europejskiej Rady Ochrony Danych Osobowych.

Jeśli zaś chodzi o sposób wyboru, to **każdy członek organu powinien zostać powołany – w drodze przejrzystej procedury** – przez parlament, rząd, głowę państwa lub niezależny organ uprawniony do powoływania członków organu nadzorczego, na podstawie przepisów państwa członkowskiego.

Kolejnym wymogiem, określonym przez RODO, jest wymóg posiadania przez członków organu nadzorczego odpowiednich **kwalifikacji**, doświadczenia i umiejętności, w szczególności w dziedzinie ochrony danych osobowych.





Wskazując na zasady ustanawiania organu nadzorczego – przepisy RODO w art. 54 określają w szczególności, zasady i procedury powoływania członków, kwalifikacje i warunki wyboru wymagane do powoływania na stanowiska członka, czy obowiązki członków lub personelu.

Zadania organów nadzorczych

RODO precyzuje także **zadania organów nadzorczych** (art. 57 RODO). Są to w szczególności:

- 1) monitorowanie i egzekwowanie stosowania RODO;
- 2) upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych;
- 3) upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich, na mocy RODO;
- 4) przyjmowanie standardowych klauzul umownych;
- 5) ustanawianie i prowadzenie wykazu związanego z wymogiem dokonania oceny skutków dla ochrony danych;
- 6) udzielanie zaleceń, dotyczących operacji przetwarzania;
- 7) rozpatrywanie skarg na przetwarzanie wniesione do organu;
- 8) zatwierdzanie kodeksów postępowania;
- 9) zajmowanie się certyfikacją w dziedzinie ochrony danych osobowych;
- 10) zajmowanie się szeroko pojętą akredytacją;
- 11) wydawanie zezwolenie na klauzule umowne;
- 12) zatwierdzanie wiążących reguł korporacyjnych;
- 13) branie udziału w pracach Europejskiej Rady Ochrony Danych.

Ogólne rozporządzenie o ochronie danych precyzuje także **uprawnienia organów nadzorczych w zakresie prowadzonych postępowań** (art. 58 ust. 1 RODO). Są to w szczególności:

- 1) nakazanie administratorowi i podmiotowi przetwarzającemu dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań;
- 2) prowadzenie postępowań w formie audytów ochrony danych;
- 3) dokonywanie przeglądów udzielonych certyfikacji;
- 4) zawiadamianie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia postanowień RODO;
- 5) uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;





- 6) uzyskiwanie dostępu do wszelkich pomieszczeń administratora i podmiotu przetwarzającego w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego.

Organy nadzorcze dysponują **szeroką paletą środków naprawczych** (art. 58 ust. 2 RODO). Mogą między innymi:

- 1) wydawać ostrzeżenia administratorowi lub podmiotowi przetwarzającemu, dotyczące możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania;
- 2) udzielać upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów RODO przez operacja przetwarzania;
- 3) nakazać administratorowi lub podmiotowi przetwarzającemu spełnianie żądanie osoby, których dane dotyczą, wynikające z przepisów RODO;
- 4) nakazać tym podmiotom dostosowanie operacji przetwarzania RODO, poprzez wskazanie sposobu i terminu;
- 5) nakazać administratorowi zawiadomienie osoby, których dane dotyczą o naruszeniu;
- 6) wprowadzić czasowe lub całkowite ograniczenie przetwarzania, w tym zakaz takiego przetwarzania;
- 7) nakazać realizację praw osób, których dane dotyczą (dotyczy sprostowania lub usunięcia danych lub ograniczenia przetwarzania danych osobowych i powiadomienie tych osób);
- 8) cofnąć certyfikację;
- 9) zastosować karę pieniężną.

Organy nadzorcze **wydają** także **zezwolenia i posiadają uprawnienia doradcze** (art. 58 ust. 3 RODO): Są uprawnione m.in. do:

- 1) udzielania porad administratorowi, zgodnie z procedurą uprzednich konsultacji;
- 2) opiniowania i zatwierdzania projektów kodeksów postępowania;
- 3) akredytowania podmiotów certyfikujących;
- 4) udzielania certyfikacji i zatwierdzania kryteriów certyfikacji;
- 5) przyjmowania standardowych klauzul umownych;
- 6) zezwalania na klauzule umowne;
- 7) zatwierdzania wiążących reguł korporacyjnych.

Jak stanowią powyższe regulacje, zakres zadań i uprawnień jest dość szeroki, co powinno w sposób kompleksowy przyczynić się do prawidłowego stosowania RODO przez uczestników rynku, a także egzekwowanie jego postanowień w przypadku niewywiązywania się z postanowień Rozporządzenia.





Osiągnij zgodność z RODO. Zostań Super IOD!

Wiedza przekazywana w przystępny sposób przez wykładowców – praktyków (możesz spotkać ich artykuły na naszym blogu ;), kameralne grupy szkoleniowe, praktyczne wzory i szablony dokumentów i procedur, egzamin zakończony wydaniem certyfikatu. To tylko niektóre z zalet naszego kursu.

Sprawdź terminy:

SPRAWDŹ

Pozycja Prezesa Urzędu Ochrony Danych Osobowych

Omówiliśmy zadania, obowiązki i uprawnienia krajowych organów nadzorczych. Jak zatem organ nadzoru przedstawia się z naszej krajowej perspektywy – **jaka jest rola Prezesa Urzędu Ochrony Danych Osobowych?**

Oczywiście, krajowy organ nadzorczy funkcjonuje w oparciu o przepisy art. 51 i następujących RODO, o których była mowa powyżej.

Status, zadania i kompetencje, zasady oraz tryb powołania regulują przepisy Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Należy pamiętać, że wiodące znaczenie mają przepisy RODO, natomiast w powyższej ustawie uregulowano te zagadnienia, które RODO przyznało państwom członkowskim, do określenia w krajowych porządkach prawnych.

Prezesa Urzędu Ochrony Danych Osobowych **powołuje Sejm za zgodą Senatu**. Wymogiem, który musi spełnić kandydat na stanowisko Prezesa UODO jest kryterium posiadania wyższego wykształcenia oraz wiedzy i doświadczenia z zakresu ochrony danych osobowych. **Kadencja** prezesa **trwa 4 lata**. Jako organ nadzorczy, Urząd Ochrony Danych Osobowych podlega wyłącznie ustawie. Prezes może powołać do trzech swoich zastępców.

Z nowych rozwiązań, które wprowadza powyższa ustawa to **ustanowienie organu opiniodawczo-doradczego – Rady do Spraw Ochrony Danych Osobowych**, której zadaniem jest m.in. opiniowanie projektów dokumentów organów i instytucji Unii Europejskiej, dotyczących spraw ochrony danych osobowych czy opracowywanie propozycji rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.

Ideą powstania tego organu była możliwość wsparcia Prezesa UODO, przez podmioty działające w różnych obszarach.



Kolejnym zadaniem Prezesa jest także m.in. **publikowanie standardowych klauzul umownych, zatwierdzonych kodeksów postępowania czy rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania.**

Ponadto Prezes UODO ogłasza **wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony.** Takie zestawienie zostało przygotowane i jest dostępne [tutaj](#).

Prezes UODO powinien także wydawać **zalecenia i wytyczne co do stosowania RODO.** Krajowy organ nadzoru opublikował kilka poradników – m.in. „Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców” czy „Jak rozumieć i stosować podejście oparte na ryzyku”. Poradniki dostępne są pod [linkiem](#).

Jest to działanie pożądane przez administratorów danych, ponieważ RODO to akt względnie nowy i jego stosowanie nastrocza w dalszym ciągu wiele kłopotów i wątpliwości.

Prezes UODO posiada także **obowiązki związane z certyfikacją i zatwierdzonymi kodeksami postępowania**, niemniej do tej pory są to mechanizmy, które nie zostały wykorzystane przez Prezesa Urzędu Ochrony Danych Osobowych.

Najbardziej jednak znanym uprawnieniem, budzącym największe emocje, **jest możliwość nakładania kar na administratorów lub podmioty przetwarzające.** Na naszym blogu prowadzimy [rejestr kar finansowych Prezesa UODO](#) wraz z kontekstem ich nałożenia oraz komentarzem ekspertów.

Procedura one stop shop

W niniejszym artykule chciałbym także poruszyć zagadnienie procedury one stop shop, która pełni dość ważną rolę wśród organów nadzorczych.

Regulacja ta została opisana w art. 60 RODO i następnych. Rozwiązanie ma i będzie miało w praktyce coraz większe znaczenie, ponieważ w dobie paneuropejskich korporacji dochodzi i będzie dochodzić do sytuacji, w których organy nadzorcze będą współpracować ze sobą wyjaśniając czy doszło na przykład do naruszenia przetwarzania danych osobowych przy transgranicznym przetwarzaniu danych osobowych, co w dobie „braku granic” w Internecie będzie z pewnością mieć miejsce.

Do maja 2018 roku w przypadku takiego transgranicznego przetwarzania, administratorzy, którzy działali w wielu krajach, musieli radzić sobie z równoległymi rozstrzygnięciami kilku krajów członkowskich. Brakowało uregulowania wymiany informacji pomiędzy poszczególnymi organami lub też wymiana ta nie była sformalizowana.

Zacznijmy od definicji **transgranicznego przetwarzania danych osobowych.**

Z takim przetwarzaniem mamy do czynienia, gdy przetwarzanie odbywa się w ramach działalności jednostek, prowadzonej w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego.

O transgranicznym przetwarzaniu mamy do czynienia wówczas, gdy mówimy o działalności polegającej na przetwarzaniu danych przez pojedynczą jednostkę organizacyjną, która znacznie wpływa, bądź może znacznie wpłynąć na osoby, których dane dotyczą w więcej niż jednym państwie członkowskim.





Od czego należy zacząć przy realizacji tej procedury?

Należy ustalić **właściwość wiodącego organu nadzorczego**, zgodnie z treścią art. 56 RODO. Jest to z reguły organ, w którym **znajduje się główna jednostka administratora lub podmiotu przetwarzającego**.

Jeśli chodzi o sytuację, w której nie mamy „głównej” jednostki administratora, a kompetencje do podejmowania decyzji rozdzielono na terytorium kilku państw członkowskich – to po stronie administratora / podmiotu przetwarzającego leży wskazanie podmiotu, który jest „główną” jednostką. Taki wybór wiąże się ze wskazaniem wiodącego organu - oczywiście organ przeprowadzi sprawdzenie, czy administrator prawidłowo wskazał gdzie (na terenie jakiego kraju) znajduje się centrum decyzyjne.

Do zadań wiodącego organu nadzorczego i organów krajowych należy wymiana informacji, które podmioty te posiadają i które mogą mieć wpływ na daną sprawę (np. informacje o przeprowadzonych wcześniej kontrolach u danego administratora danych).

Wiodący organ nadzorczy niezwłocznie przekazuje innym organom nadzorczym, biorącym udział w postępowaniu, **stosowne informacje dotyczące danej sprawy, niezwłocznie przedkłada im projekt decyzji w celu uzyskania ich opinii i należytego uwzględnienia ich uwag**.

Jeżeli w terminie czterech tygodni od otrzymania wniosku o opinię inny organ nadzorczy, którego sprawa dotyczy, zgłosi mający znaczenie dla sprawy i uzasadniony sprzeciw wobec projektu decyzji, wiodący organ nadzorczy – jeżeli nie przychylił się do sprzeciwu – przekazuje sprawę w ramach mechanizmu spójności. Jeżeli wiodący organ nadzorczy zamierza przychylić się do uzasadnionego sprzeciwu, przedkłada innym organom nadzorczym, zmieniony projekt decyzji.

W tym miejscu warto wspomnieć, że w procedurze tej może uczestniczyć również Europejska Rada Ochrony Danych - zgodnie z treścią art. 65 ust. 1 RODO sprawa przekazywana jest EROD, która wydaje w jej sprawie wiążącą decyzję w przypadku, gdy organ nadzorczy, którego sprawa dotyczy, zgłosił uzasadniony sprzeciw wobec projektu decyzji wiodącego organu nadzorczego, a wiodący organ nadzorczy odrzucił taki sprzeciw.

Wspólne operacje

W przypadku realizacji działań wykonywanych w ramach procedury – może **dojść do wspólnych operacji**. Z reguły taka sytuacja będzie mieć miejsce, gdy organ nadzorczy będzie potrzebował wykonać jakieś działanie przy pomocy innego organu nadzorczego (np. na terytorium innego państwa członkowskiego). W praktyce, czynności na terytorium danego państwa członkowskiego, może dokonywać wyłącznie organ nadzorczy tego państwa, bądź wyjątkowo organ innego państwa, jednak pod kierownictwem pracowników przyjmującego organu nadzorczego. Należy wspomnieć, że przyjmuje się, że wspólne operacje to nie obowiązek, lecz uprawnienie, z którego może korzystać organ nadzorczy - a jego celem jest ułatwienie wyjaśnienia sprawy, którą zajmuje się organ wiodący.

Mechanizm spójności

Jednym z ostatnich zagadnień jest **wprowadzenie mechanizmu spójności** – pomiędzy organami nadzorczymi, Europejską Radą Ochrony Danych, a Komisją Europejską.

Istotą sprawy jest współpraca administracyjna w celu zapewnienia jednolitości stosowania w odniesieniu do operacji przetwarzania, które mogą dotyczyć podmiotów danych w kilku państwach członkowskich.





Nadmienić należy, że również Europejska Rada Ochrony Danych ma w tym zakresie określone kompetencje – wydaje opinie, gdy dany organ nadzorczy zamierza wykonać m.in. następujące operacje - przyjęcie operacji przetwarzania, zatwierdzenie czy projekt, bądź zmianę kodeksu, zatwierdzenie wiążących reguł korporacyjnych.

Kompetencje i zadania EROD (w tym również działania w ramach mechanizmu spójności) będą przedmiotem odrębnego artykułu.

Wydawać by się mogło, że procedura one stop shop jest mechanizmem, który nie jest wykorzystywany przez organy nadzorcze. Jednak, jak się okazuje, w chwili obecnej EROD opublikował ponad 110 wspólnych decyzji w ramach one stop shop.

W wykazie tym nie ma polskiego organu nadzorczego, jako organu wiodącego, natomiast UODO występuje jako uczestnik w postępowaniach w ramach one stop shop. Rejestr dostępny jest [tutaj](#).

A zatem jest to narzędzie wykorzystywane przez europejskie organy nadzoru i można przypuszczać, że rola procedury one stop shop będzie się zwiększała.

Podsumowanie

Celem artykułu było bliższe przyjrzenie się kompetencjom krajowych organów nadzorczych (ich zadaniom czy uprawnieniom), w tym kontekście omówiliśmy pozycję Prezesa Ochrony Danych Osobowych (procedurę powołania, wymagania i główne zadania jakie stoją przed Prezesem). Ostatnim zagadnieniem, które poruszył artykuł to mechanizm one stop shop, który powinien ułatwiać działanie organów nadzorczych przy transgranicznym przetwarzaniu danych osobowych. Mamy nadzieję, że udało się uporządkować informacje, o tych niezbyt często w praktyce poruszanych tematach, które jednak mają istotne znaczenie przy stosowaniu RODO.

Autor artykułu:

Krystian Dobosz, starszy specjalista ds. ochrony danych osobowych

Źródła:

- [Rozporządzenie Parlamentu Europejskiego i Rady \(UE\) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE \(Ogólne rozporządzenie o ochronie danych\) – RODO](#)
- [Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych \(Dz. U. 2018 poz. 1000 ze zm.\)](#)
- Edyta Bielak-Jooma (red.), Dominik Lubasz (red.) RODO. Ogólne rozporządzenie o ochronie danych. Komentarz. WKP 2018
- P. Litwiński (red). Rozporządzenie UE w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Wydawnictwo C.H. Beck, 2018

