



NAJCZĘSTSZE PROBLEMY W DZIAŁALNOŚCI IOD

Zapis debaty, która odbyła się 28 stycznia 2020 r. podczas Dnia Otwartego w UODO, zorganizowanego z okazji XIV Dnia Ochrony Danych Osobowych

W debacie udział wzięli: Mirosław Sanek, Zastępca Prezesa Urzędu Ochrony Danych Osobowych, dr Grzegorz Sibiga z Instytutu Nauk Prawnych PAN, Monika Młotkiewicz, naczelnik Wydziału Współpracy z IOD w UODO oraz Piotr Drobek, radca, UODO. Debatę prowadził Adam Sanocki, Rzecznik Prasowy UODO.

Adam Sanocki: Z jakimi problemami w minionym roku inspektorzy najczęściej się do nas zgłaszali?

Monika Młotkiewicz: Inspektorzy ochrony danych od dawna wiedzą, że mają prawo zwracać się do nas z pytaniami i nie wahają się z tego prawa korzystać. Rok 2019, podobnie jak rok 2018, był czasem bardzo istotnych zmian w dziedzinie ochrony danych osobowych. W 2018 roku rozpoczęliśmy stosowanie RODO, a w 2019 roku weszła w życie ustawa wdrażająca tzw. dyrektywę policyjną oraz duży pakiet zmian w związku z wejściem w życie tzw. ustawy wdrażającej RODO w Polsce.

Pytania od inspektorów ochrony danych odzwierciedlały ich wątpliwości związane z tymi zmianami. Inspektorzy pytali nas np. jak realizować obowiązki wynikające z tych przepisów, gdy w ramach jednej struktury organizacyjnej – sądu albo urzędu gminy – funkcjonuje kilku administratorów danych. Przykładowo takimi administratorami są: sąd jako jednostka organizacyjna, dyrektor sądu, prezes sądu, czy - w przypadku urzędu gminy - oprócz organów wykonawczych i uchwałodawczych samorządu takim administratorem jest komendant straży gminnej. Zadawane były szczegółowe pytania o obo-

wiązki związane z wewnętrznymi politykami czy inną dokumentacją taką jak rejestr czynności.

Cały czas - i tak było również w 2019 roku - otrzymujemy pytania o charakterze zasadniczym tzn. jaki podmiot należy uznać za administratora danych. Pytano nas np. czy biegli rewidenci w związku ze świadczeniem swoich usług mają taki status. Było pytanie dotyczące np. charakteru rady rodziców czy różnych komisji, które działają przy poszczególnych organach, np. komisji ds. orzekania o zdarzeniach medycznych. Jak w przypadku takich podmiotów podchodzić do ich statusu.



Monika Młotkiewicz

Wiele pytań dotyczyło też umowy powierzenia danych: czy należy ją zawierać w określonych sytuacjach, np. czy pracodawca jest zobowiązany zawierać umowy powierzenia z urzędem skarbowym, Głównym Urzędem Statystycznym, Zakładem Ubezpieczeń Społecznych lub bankiem. Albo czy taką umowę powierzenia powinna zawierać szkoła z ośrodkiem pomocy społecznej.

Mieliśmy też dużo szczegółowych pytań dotyczących obowiązków wynikających zarówno z RODO, jak i z ustawy wdrażającej dyrektywę policyjną, np. dotyczące upoważnień i formy ich wydawania, komu powinny być udzielane, czy takich upoważnień należy udzielać np. sędziom, czyli osobom, których uprawnienie do przetwarzania danych wynika z przepisów prawa. Przepisy sektorowe wprowadziły zmiany dotyczące upoważnień i wątpliwości inspektorów były z tym związane.

To były ważne pytania, świadczące o tym, że inspektorzy bardzo szybko identyfikują problemy prawne i oczekują od urzędu pewnych wskazówek.

Na większość pytań, o których powiedziałam, można znaleźć odpowiedzi na naszej stronie internetowej, zarówno w zakładce poświęconej inspektorom ochrony danych, jak i w newsletterze, który w ubiegłym roku rozpoczęliśmy wydawać jako specjalny biuletyn dla IOD.

Adam Sanocki: Mamy też infolinię, gdzie z tymi pytaniami także inspektorzy do nas się zgłaszają. Panie Ministrze, jak Pan widzi rolę Urzędu? Jakie elementy uważa Pan za najważniejsze w kontaktach z IOD?

Mirosław Sanek: Najogólniej rolą UODO jest współpraca, która zresztą jest także wpisana w obowiązki inspektorów ochrony danych. Przy czym jest to pojęcie bardzo szerokie, mające swoje tradycje jeszcze przed RODO i na tyle pojemne, że zaprasza nas do jego twórczego uzupełniania. I to staramy się aktywnie czynić, dostarczając merytorycznych treści, ujednolicających praktykę stosowania tego niewątpliwie trudnego aktu prawnego jakim jest RODO, stanowiącego samo w sobie duże wyzwanie w jego interpretacji.

Urząd od dłuższego czasu oczywiście nie czeka biernie na realizację tego zadania. Padło tutaj kilka przykładów sposobów komunikacji, jak: newsletter, infolinia, prowadzimy także sektorowe szkolenia, które mają tę ważną cechę i skutek, że doprowadzają do ujednolicenia rozumienia niektórych zapisów.

Oprócz materiałów szkoleniowych, szkoleń sektorowych dla inspektorów ochrony danych, oprócz tych kanałów

komunikacyjnych, niezmiernie ważnych dla obu stron, bo dla nas to też jest sygnał, gdzie pojawiają się problemy ponadjednostkowe, gdzie możemy reagować, to trzeba też powiedzieć o sposobie reakcji ogólnej. To przede wszystkim tematyczne wytyczne i poradniki, które sukcesywnie UODO przygotowuje i prezentuje.

Mam nadzieję, że ilekroć tego typu materiał się pojawi, możemy liczyć na państwa bardzo pozytywną reakcję w jego odbiorze i promocji. Bardzo na to liczymy. Odpowiadając jeszcze raz na to pytanie, Urząd przede wszystkim musi dbać o podnoszenie fachowości IOD oraz jednolitość stosowania ogólnego rozporządzenia.

Adam Sanocki: Panie Doktorze, jakimi cechami Pana zdaniem powinien wyróżniać się wzorcowy IOD, poza tym, że powinien zadawać, i zadaje, dużo pytań, czyli jest dociekliwy?

Dr Grzegorz Sibiga: Pozwolę sobie na to pytanie odpowiedzieć z punktu widzenia własnych doświadczeń, ponieważ mam przyjemność kierować w INP studiami podyplomowymi, przeznaczonymi właśnie dla IOD, zresztą pod patronatem UODO, za który dziękujemy. Również wspieram jako ekspert stowarzyszenie IOD, więc pozwolę sobie przekazać Państwu swoje uwagi i rozważenia na ten temat.



Mirosław Sanek

Samo RODO i wyjaśnienia do niego określają, że podstawowym warunkiem dla IOD jest wymóg wiedzy fachowej, dotyczącej przede wszystkim znajomości przepisów o ochronie danych osobowych. A przypomnę, że są to nie tylko RODO i „przepisy policyjne”, ale bardzo duża grupa aktów uzupełniających ogólne rozporządzenie. W naszym kraju mamy przecież do czynienia z kilkaset aktami prawnymi na poziomie ustaw i rozporządzeń do nich, które w jakiś sposób regulują kwestie przetwarzania i ochrony danych osobowych.

Ale ta wiedza, dotycząca samego prawa, nie jest wystarczająca. To bardzo wyraźnie również wskazano w wytycznych, że ta wiedza powinna być połączona

ze znajomością specyfiki własnej organizacji lub jednostki organizacyjnej, z jej kulturą organizacyjną czy pracy.

W związku z tym w administracji publicznej IOD powinien znać strukturę wewnętrzną, zasady dotyczące funkcjonowania, procedury, które występują w urzędzie. Z kolei IOD w sferze prywatnej, powinien znać swój biznes, wiedzieć na czym on polega, gdzie są te dane osobowe, jakie problemy są z nimi związane.

Czyli wiedza powinna dotyczyć dwóch aspektów, zarówno prawnego, jak i praktyki związanej ze swoim urzędem, czy ze swoją firmą.

Natomiast chciałbym Państwu zwrócić uwagę na coś, co być może tak często nie jest podkreślane. Otóż dla mnie wzorcowy IOD powinien rozumieć swoją rolę. Rozumieć na czym polega jego funkcja w jednostce organizacyjnej. Uwaga! Nie jest to funkcja obrońcy. Obrońcy w tym znaczeniu, że „bronię cokolwiek mój urząd/ moja firma wdrożyła, przetwarza dane osobowe i ja mam być tym, który spróbuje obronić teraz to rozwiązanie np. przed UODO albo przy roszczeniach osób, których dane dotyczą”.

Właściwą rolę IOD jest dbanie o wysoki standard realizacji prawa do ochrony danych osobowych. To jest jego kierunek, któremu podporządkowane powinny być te wszystkie działania, o których mówi RODO, czyli informowanie, doradzanie, monitorowanie. „Moim zadaniem jako inspektora jest zapewnienie jak najwyższego standardu. Patrząc na to z punktu widzenia prawa do ochrony danych osobowych i staram się, żeby to było komplementarne z działalnością, którą prowadzi moja jednostka organizacyjna”. Dlatego też – co dla w naszej działalności w Instytucie Nauk Prawnych jest tak ważne – oprócz przedmiotów, takich ściśle zawodowych, dotyczących wykonywania obowiązków, warsztatu pracy, bardzo ważnym przedmiotem jest etyka wykonywania tej funkcji. Właściwe zrozumienie i etyczne podejście, choćby z punktu widzenia właściwego rozumienia niezależności, niepodlegania wpływom i rozumienia swojej roli, swojej funkcji w organizacji.

Adam Sanocki: Czy w związku z tym kompetencje IOD powinny być poparte jakimś egzaminem? Dużo się mówi ostatnio o certyfikacji inspektorów?

Piotr Drobek: W środowisku inspektorów toczy się dyskusja, jak można urzędowo potwierdzać kompetencje, bądź wiedzę inspektorów ochrony danych. Żeby odpowiedzieć na to pytanie, musimy pamiętać o jednej rze-

czy, że zawód – nie bójmy się tego sformułowania, bo to już nie jest tylko osoba pełniąca funkcję – szczęśliwie wykształca się na naszych oczach bardzo ważny zawód w naszym społeczeństwie.



Piotr Drobek

Ten zawód nie ma charakteru zawodu regulowanego. To nam wyłącza możliwość urzędowego potwierdzenia kompetencji, bądź też wprowadzania urzędowych egzaminów, od których uzależnione byłoby wykonywanie tego zawodu. Tak ukształtowany został status IOD na gruncie RODO i na pewno na poziomie krajowym tych regulacji zmienić nie możemy. Nie możemy też w inny sposób ich ukształtować, niż zostały one ukształtowane na poziomie unijnym.

Musimy pamiętać, że to jest zawód wykonywany nie tylko w Polsce, ale musimy na ten zawód patrzeć z perspektywy całego jednolitego rynku. I z tego bardzo się cieszymy, że już wielu polskich inspektorów na tym rynku funkcjonuje i to z dużym powodzeniem. Z drugiej strony to oznacza, że polscy inspektorzy są wystawieni na konkurencję inspektorów z innych krajów. To też pozwoli zaczynać zauważać w naszym kraju.

Nie jest to zawód regulowany, a cały czas jednak pojawia się potrzeba jakiejś formy potwierdzenia, bądź też potrzeba istnienia takiej ścieżki, żeby każdy inspektor, każda osoba, która chce wykonywać ten zawód też wiedziała, czego powinna się nauczyć, jakie umiejętności powinna zdobyć, żeby być dobrym w czasie wykonywania tej funkcji.

Mamy tutaj różne możliwości. Jedną z nich rzeczywiście mogłaby być certyfikacja, ale z zastrzeżeniem, że certyfikacja o charakterze dobrowolnym.

Od razu dodajmy, że to nie będzie certyfikacja w rozumieniu RODO, bo ono nie dopuszcza certyfikacji osób. Czyli mówimy o innych dobrowolnych mechanizmach certyfikacji, które funkcjonują w bardzo różnych obszarach życia społeczno-gospodarczego. We Francji

i w Hiszpanii na podstawie krajowych przepisów oba organy nadzorcze stworzyły programy certyfikacji inspektorów ochrony danych. Same te organy nadzorcze nie certyfikują, ale stworzyły ramy, na podstawie których taka certyfikacja może się odbywać. Ale jeszcze raz podkreślam, certyfikacja o charakterze dobrowolnym.

Możliwe też jest podejście, w ramach którego – myślę, że ono jest dużo bardziej realne w tej chwili – jest praca środowisk i organizacji zrzeszających IOD. W tej chwili mamy kilka organizacji i te organizacje mają bardzo ważną rolę do odegrania w stworzeniu standardów, nie tylko etycznych. To jest jedna z ważniejszych kwestii. Ale też wydaje mi się, że organizacje zrzeszające inspektorów ochrony danych powinny odegrać bardzo ważną rolę w podnoszeniu kompetencji swoich członków, wskazując ten kierunek, tworząc ramy do tego, żeby członkowie mogli podwyższać swoje kompetencje.

Teraz powinniśmy na te różne rozwiązania patrzeć w sposób komplementarny. Czyli z jednej strony organizacji, z drugiej strony, mogą się pojawić mechanizmy certyfikacji, które nie mogą w swoim założeniu blokować dostępu do wykonywania tego zawodu. I to też musimy podkreślić, de iure bądź de facto. Analizujemy tą sytuację i będziemy się zastanawiać nad tym, czy UODO powinien aktywniej podejmować działania. Musimy pamiętać o tym, że to nie może wydarzyć się z dnia na dzień, bo tworzenie zawodu też trwa od 2015 roku.

Myślę, że wszyscy możemy się zgodzić, że ta grupa zawodowa bardzo się profesjonalizowała. Mamy bardzo dużą grupę ludzi, którzy w tej chwili są bardzo dobrymi ekspertami. I w tym sensie, budując świadomość tej grupy i ich kompetencje, też powinniśmy wykorzystywać wszystkie dostępne instrumenty.

Adam Sanocki: UODO bardzo często podkreśla, że inspektor ochrony danych powinien być skuteczny i niezależny. Tu rodzą się dwa pytania. Co to oznacza? Dlaczego to jest takie ważne?

Mirosław Sanek: Zacznę od powiedzonka, które jest oczywiste, że „nie ma w tym zawodzie skuteczności bez niezależności”. Dlatego skupię się na niezależności jako warunku dla skuteczności inspektora.

Oczywiście niezależność to jest takie pojęcie, które wszyscy rozumiemy po swojemu, bo jest to wstęp do potocznego rozumienia tego pojęcia, które jest w końcu pojęciem prawnym. Z drugiej strony, gdy czytamy odpowiedni artykuł regulujący status IOD mamy tam dużo więcej

konkretów, niż tylko jedno pojęcie okołoprawne. Szybko możemy dojść do wniosku, że tak naprawdę potocznie rozumiana niezależność jest trochę mocniejsza niż niezależność w statusie fundowanym na gruncie RODO. Niewątpliwie jest to niezależność merytoryczna. Tak jak Pan Doktor bardzo barwnie i syntetycznie nakreślił rolę inspektora, tutaj możemy mówić o pełnej, pożądanej niezależności oraz ogólnie o autonomii inspektora w organizacji. Mówimy oczywiście o podległości służbowej, pracowniczej w stosunku pracy, ale też o dystansie, ulokowaniu. Musi być to bezpośrednie podleganie najwyższemu kierownictwu.

Natomiast pamiętajmy, że zapewnienie niezależności merytorycznej inspektora, jest obowiązkiem administratora, również ujętym w artykule 83, czyli w regulacji administracyjnej kary pieniężnej. Oczywiście jest to ten niższy pułap, aczkolwiek nawet niższy pułap robi wrażenie.

Na czym polega to zapewnienie? To jest przede wszystkim zapewnienie niezwłocznego dostępu do spraw dotyczących danych osobowych, które intuicyjnie wszyscy rozumiemy, ale z pewnością wymaga pogłębienia. Na szczęście wytyczne wyszczególniają te perspektywy niezwłocznego dostępu.

Po pierwsze musi być dostęp, o czym się zapomina, bo przechodzi się do kwestii merytorycznych, dla wszystkich pracowników i osób związanych z organizacją. Muszą wiedzieć, że taka postać jak inspektor działa i ma takie a nie inne obowiązki, taki a nie inny status. Jesteśmy w tej sytuacji, jak mówił Pan Piotr Drobek, że każdy może być inspektorem ochrony danych. W pewnym sensie każdy, natomiast dopiero potem pojawiają się ogólne warunki jak fachowość, dostępność.

Drugim pułapem jest dostępność do danych osobowych, przetwarzanych w organizacji. A trzecim, bardzo istotnym i właściwie będącym nerwem niezależności inspektora, to jest dostęp do możliwości opiniowania projektowanych procesów na danych osobowych. Nie ma niezależności bez zapewnienia dostępu inspektora do tych trzech sfer.

Aczkolwiek najistotniejsze w tym obowiązku jest zapewnienie stałego rozwoju fachowości, merytoryczności inspektora.

Świat nam się bardzo gwałtownie rozwija. Zadania w zakresie obowiązku IOD są zadaniami dynamicznymi. Poprzeczka idzie w górę, a więc administrator, który nie zapewnia, nie przywiązuje należytej wagi do stałego,

realnego rozwoju merytorycznego swojego IOD również naraża się na zarzut, że tego obowiązku nie realizuje.

Wszyscy tutaj chwaliliśmy IOD, mówiliśmy już, że jest to zwarty zawód, który prezentuje poziom merytoryczno-organizacyjny w swoich jednostkach, aczkolwiek też jesteśmy w stanie mówić o sytuacjach niepokojących. Oczywiście wynikających z tego, że każdy może być IOD. Niektórzy administratorzy myślą, że to naprawdę każdy dowolny. Wystarczy wziąć kogoś z zewnątrz, a więc ta osoba od razu, na wstępie już, nie spełnia tego warunku, że może i zna prawo, ale nie zna kultury organizacyjnej w jednostce. Jednym z wielu zadań Urzędu jest także przeciwdziałanie takim niepokojącym zjawiskom. Bardzo chcielibyśmy, by inspektorzy byli tym środowiskiem, które jest realnym, aktywnym wsparciem dla zadań spoczywającym na Prezesie Urzędu.

Dr Grzegorz Sibiga: Jeżeli mogę uzupełnić o tą drugą cechę, bardziej kryterium skuteczności, to muszę powiedzieć, że jest to niezwykle trudne pytanie, ponieważ pamiętajmy o tym, że IOD nie ma takiego władztwa. On tylko doradza. On tylko informuje administratora o prawidłowym sposobie wykonania przepisów. To administrator podejmuje decyzje – i uwaga – może nie uwzględnić sugestii IOD. Rekomendacja IOD może nie mieć zatem wpływu na to, co dzieje się faktycznie z danymi osobowymi.

Również wydaje się, że tym kryterium nie może być np. ocena, czy doszło/dochodzi w jednostce czy nie do naruszeń ochrony danych osobowych. Bo im większa skala przetwarzania, im większy stopień wykorzystania nowych technologii, tym większa prawdopodobieństwo zaistnienia naruszenia. Nawet wprowadzając szereg działań prewencyjnych, możemy nie uniknąć pewnych zdarzeń, w dużej części od nas niezależnych.

Dla mnie tym kryterium skuteczności, jak liczyć tę skuteczność, będzie kompleksowość podjętych działań. Czyli, w jakim stopniu IOD ma wiedzę o wszystkich procesach związanych z przetwarzaniem danych osobowych, które mają miejsce w jednostce organizacyjnej i w ramach tych wszystkich procesów wypowiada się, rekomenduje określone wykonanie obowiązków.

Natomiast z tym pytaniem o skuteczność jest związane też bardzo duże wyzwanie na przyszłość. O co chodzi? Otóż pamiętajmy, że przepisy RODO mówią, że IOD powinien uwzględniać w swojej działalności ryzyko związane z operacjami przetwarzania danych osobowych. Czyli nie tylko administrator, ale też inspektor działa

na zasadzie analizy ryzyka – z punktu widzenia nie tylko praw podmiotów danych osobowych, ale już to ryzyko uwzględniające operacje przetwarzania danych osobowych, to jest również ryzyko dla jednostki organizacyjnej. Dlaczego mówię o tym wyzwaniu? Ponieważ nie ma na razie jednolitego podejścia, co oznacza uwzględnienie ryzyka w działalności IOD, a właściwa analiza ryzyka, może się przekładać na skuteczność. To jest duże wyzwanie, zarówno przed Urzędem, jak i przed specjalistami, żeby spróbować odpowiedzieć na pytanie: w jaki sposób inspektor powinien analizować ryzyko w swojej działalności.



Dr Grzegorz Sibiga

Monika Młotkiewicz: Skuteczność definiuje się jako sprawianie, że rzeczy się dzieją. Ale to, jak już tu było podkreślane, jest zadaniem całej organizacji – administratora, czyli kierownictwa i podległych mu pracowników. Dlaczego o tym mówię? Dlatego, że wydaje mi się, iż w Polsce jeszcze w wielu miejscach niestety potuluje błędne przekonanie, że ochrona danych osobowych to jest zmartwienie, praca tylko jednej osoby – inspektora ochrony danych, a tak nie da się zapewnić właściwej ochrony danych. Potrzebny jest systemowy i systematyczny wysiłek wszystkich, którzy z danymi osobowymi mają do czynienia, zwłaszcza tych, którzy instytucją zarządzają i za jej działanie są odpowiedzialni. Skutecznego inspektora należy natomiast postrzegać jako strażnika, kogoś takiego, kto pilnuje, żeby „rzeczy się działy”, tzn. że np. uprawnienia osób są terminowo i faktycznie respektowane lub procedury w zakresie poufności są przestrzegane. Jeżeli u administratora jest autentyczny, skuteczny system ochrony danych osobowych, funkcjonujący zgodnie ze standardami, to dostrzegają to klienci i partnerzy biznesowi, a także my - pracownicy UODO, prowadząc różne postępowania. Widzimy od razu, czy inspektor nie jest osamotniony w swoich zmaganiach o zapewnienie przestrzegania przepisów oraz celowo pomijany w codziennej działalności administratora, tak, że nikt nie zwraca się do niego o opinię. To są ważne kryteria oceny administratora przez podmioty zewnętrzne, w tym podmiot nadzorujący.

Jeśli chodzi o niezależność inspektora, to warto podkreślić rolę strażnika przestrzegania praw jednostki. Bo ochrona danych osobowych to jest wycinek szerszej dziedziny jaką są prawa człowieka. Obserwujemy, że wielu inspektorów bardzo dobrze to rozumie, tzn. oni wiedzą, gdzie są zagrożenia, ryzyka dla tych praw np. w niewłaściwym rozumieniu niektórych przepisów i to jest ważne, jeśli chodzi o skuteczność i niezależność inspektora.

Piotr Drobek: Po jednym z wykładów poza Warszawą, jedna ze słuchaczek powiedziała tak: Proszę państwa, oglądałam wasze szkolenia, jedno, drugie, one pokazują świat idealny. One powinny pokazywać wzór, do którego powinniśmy dążyć. I później usłyszałem historie, jakie problemy ta osoba ma w trakcie wykonywania funkcji IOD, głównie dlatego, że kierownik jednostki, w której funkcjonuje, jednostki publicznej generalnie, nie rozumie obowiązków wynikających z przepisów o ochronie danych. Nie rozumie roli IOD oraz nie chce zapewnić odpowiednich zasobów.

Z tej perspektywy, to było już powiedziane, jak możemy ocenić skuteczność takiej osoby. Oczywiście IOD działa w tym środowisku, w którym jest, mając świadomość ograniczeń, które w tej organizacji występują. Ale na pewno skutecznym inspektorem nie będzie osoba, która funkcjonuje w ramach jakiejś tylko „bezludnej wyspy ochrony danych”, zupełnie nie komunikując się z organizacją. Dlaczego? Bo tutaj, nawet jeżeli doradza, eliminuje jakąkolwiek możliwość wpływania, bądź przekonywania do tego, że określone rozwiązania mogą być ważne. To oznacza, że IOD, aby być skutecznym, musi potrafić komunikować się z członkami organizacji, przede wszystkim z kierownictwem, ale również z innymi osobami. Jak popatrzymy na organizacje, które pozytywnie oceniamy, to się okazuje, że tam właśnie był aktywny, komunikujący się IOD, który nie zawsze wygrywa swoje walki o to, żeby zachować standard, ale na pewno dąży do tego, aby ten standard był jak najwyższy. Nie chcę powiedzieć, że walczy o to każdego dnia, ale buduje dzień po dniu kulturę ochrony danych osobowych w organizacji.

Adam Sanocki: **Bardzo proszę o kilka zdań podsumowania. Jest jeszcze styczeń, to dobry moment, żeby zapytać o wyzwania na obecny, 2020 rok. Jakie Państwo widzicie wyzwania dla IOD półtora roku po rozpoczęciu stosowania RODO? Co uważacie Państwo za najważniejsze w tym roku z tej perspektywy?**

Monika Młotkiewicz: Moim zdaniem, ogromnym wyzwaniem jest wytrwałe kontynuowanie tej codziennej

pracy w zakresie przestrzegania prawa ochrony danych osobowych. Tutaj mówimy o długofalowych działaniach i to działaniach wszystkich osób przetwarzających dane w organizacji. Natomiast zadaniem inspektora jest cały czas budowanie, a następnie podtrzymywanie świadomości - w kontekście zmieniających się wraz z postępem technologicznym standardów – w zakresie obowiązków w dziedzinie ochrony danych osobowych. Nieatrakcyjnie zabrzmiało to co powiem, ale chodzi tak naprawdę o konsekwencję, systematyczność i cierpliwość w wykonywaniu tej pracy, a to jest duże wyzwanie.

Piotr Drobek: Spojrzę na to z innej strony. Wyzwaniem na ten rok i myślę, że na kolejne, jest ciągłe budowanie pozycji inspektora ODO w organizacjach. Budowanie świadomości wśród administratorów i podmiotów przetwarzających, w świadomości najwyższego kierownictwa, że ochrona danych osobowych, to nie jest jedynie zadanie osoby do tego wyznaczonej, czyli IOD, ale przede wszystkim odpowiedzialność administratora, bądź podmiotu przetwarzającego. To zmienia zupełnie postrzeganie roli i zadań IOD. Bo jeżeli „nie zwalniam się z tej odpowiedzialności, to lepiej muszę wybierać, lepiej muszę rozumieć potrzebę wspierania tej osoby”.



I wydaje mi się, że to jest jedno z najważniejszych zadań przed nami wszystkimi, nie tylko przed inspektorami, żeby budować tę świadomość i tak, żebyśmy mogli za kilka lat, analizując stan ochrony danych osobowych, stwierdzić, że jednak w większości organizacji ta świadomość jest na wysokim poziomie.

Dr Grzegorz Sibiga: Oczywiście zgadzam się z moimi przedmówcami, tylko uzupełnię, nie powtarzając już tych bardzo trafnych ich spostrzeżeń. Podzieliłbym wyzwania na merytoryczne, związane z pewnymi obszarami merytorycznymi działalności IOD i wyzwania dotyczące samego wykonywania funkcji. Na pewno wyzwaniem merytorycznym jest stale zwiększające się znaczenie i zastosowanie nowych technologii przetwarzania danych. To rodzi problemy techniczne, związane z wiedzą, ze zrozumieniem tych technik, bo żeby w czymś doradzać, trzeba zrozumieć, orientować się w tej materii.

Innym takim wyzwaniem dla sektora publicznego rozumie jest styk między otwartością z jednej strony administracji i otwieraniem przez nią danych, jawnością jej działalności, a z drugiej strony ochroną danych osobowych, również rozumianą jako ochronę poufności tych danych. No i tutaj nasz kraj, tak jak inne państwa członkowskie jest przed dużym wyzwaniem, ponieważ czeka nas wdrożenie nowej dyrektywy unijnej o otwartych danych i o ponownym wykorzystywaniu informacji sektora publicznego. Czyli ten styk jest niezwykle trudny, są to dwa rodzaje obowiązków, które kolidują ze sobą, z jednej strony udostępniania, otwierania, z drugiej strony ochrony danych.

Wreszcie wyzwaniem merytorycznym jest stale zwiększająca się liczba przepisów normujących przetwarzanie i ochronę danych, ponieważ prawna regulacja ochrony danych osobowych to nie tylko RODO. Obowiązuje spora i stale powiększająca się grupa przepisów krajowych, ale również UE, dotycząca ochrony danych osobowych. Jak te problemy przekładają się na wykonywanie swoich zadań przez samego inspektora? Wymagana jest ciągła potrzeba doskonalenia, zwiększania swoich kompetencji w tym zakresie. Razem oczywiście to trzeba traktować łącznie z tymi zadaniami, z tymi kierunkami,

o których mówili moi szanowni przedmówcy. To bym widział jako wyzwanie dla IOD w 2020 roku.

Mirosław Sanek: Wygląda na to, że nie ma co szukać specjalnie nowych wyzwań na kolejny rok, skoro wszystkie wymienione bardzo istotne i trafne wyzwania są dziedziczone po latach 2018 i 2019. Są one na tyle istotne, że faktycznie skupimy się na nich. Dobrze, że nam nic nowego nie przybywa, że najwyższej ich skala rośnie.

Pozwolę sobie na jeden slogan na podsumowanie. Nie slogan, coś bardzo prawdziwego, w co wierzymy w Urzędzie, jakość i realny status IOD to jest podstawa do tego, by oceniać reformę ochrony danych, jej intensywność, głębokość, czy nie daj Boże płytkość, to się nam już wkrótce okaże.

Pierwszy okres kilkuletni będzie najistotniejszy, obserwując zaangażowanie inspektorów oraz działalność środowisk ich skupiających. Obserwując cały rynek, który wokół tego się tworzy, bardzo kibicuję podniesieniu jakości na tym terenie i jest to dla mnie podstawa do tego, by być zdrowym, umiarkowanym w polskim duchu tego słowa optymistą.

Prezes Urzędu Ochrony Danych jest niezależnym, centralnym organem administracji publicznej ustanowionym w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii. Do jego zadań należy także m.in. upowszechnianie w społeczeństwie wiedzy z zakresu ochrony danych osobowych, upowszech-

nianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach na nich spoczywających czy monitorowanie i egzekwowanie stosowania przepisów RODO.

Chcesz wiedzieć więcej, wejdź na stronę internetową www.uodo.gov.pl lub skontaktuj się z Urzędem za pośrednictwem infolinii **606 950 000**.

