GIODO: powszechne dopuszczenie biometrii nie wpłynie na lepszą ochronę danych

09.11.17

Mam wątpliwości co do pozyskiwania danych biometrycznych, czy powszechne dopuszczenie biometrii będzie wiązało się z ochroną danych - mówi dr Edyta Bielak-Jomaa, Generalny Inspektor Ochrony Danych Osobowych.


Własne

Rozmowa z dr Edytą Bielak-Jamaa, Generalnym Inspektorem Ochrony Danych Osobowych.

- Czy RODO jest bardziej represyjne w stosunku do biznesu, czy raczej pozwala biznesowi na poluzowanie rygorów?
- Kształt unijnego ogólnego rozporządzenia o ochronie danych (RODO) to efekt wielu dyskusji zakończonych kompromisem, w wyniku którego z jednej strony wzmocnione zostały prawa obywateli, z drugiej zaś zwiększono obowiązki i odpowiedzialność administratorów danych, lecz dano im większą elastyczność działania. Przykładowo przedsiębiorca, który pozyskuje i wykorzystuje mniejsze ilości danych i robi to przy użyciu tradycyjnych środków, nie musi spełniać wielu rygorów, które ciążą na tych, którzy przetwarzają np. wiele danych, i to szczególnej kategorii, a dodatkowo wykorzystują w tym celu zaawansowane rozwiązania informatyczne. Co ważne, RODO to podstawowy akt prawny, który określa jednolite zasady przetwarzania danych osobowych we wszystkich państwach członkowskich Unii Europejskiej. Zdecydowanie zmienia podejście do ochrony danych osobowych, opierając je

na szacowaniu ryzyka i zasadzie rozliczalności. Oznacza to, że od 25 maja 2018 r., czyli od dnia rozpoczęcia stosowania tych nowych przepisów, każdy administrator danych – biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych – będzie musiał samodzielnie zdecydować, jakie zabezpieczenia, dokumentację i procedury przetwarzania danych wdrożyć.
Niebezpieczne poluzowanie rygorów nałożonych na administratorów danych dostrzegam natomiast w projektach ustaw przygotowanych przez Ministerstwo Cyfryzacji, zwłaszcza zaś w tym, mocą którego zmianie ma ulec wiele przepisów branżowych.

- Czy projekt ustawy wykroczy poza ramy RODO?
- To, co nas niepokoi, to bardzo liczne propozycje różnego rodzaju wyłączeń. Projektodawca zbyt często posługuje się prostym sformułowaniem „przepisów rozporządzenia nie stosuje się", nie podając żadnego racjonalnego, a ponadto zgodnego z RODO uzasadnienia takich wyłączeń (zgodnego, czyli zapewniającego odpowiednie gwarancje dla osób, których prawa są ograniczane). A mowa tu o zniesieniu konieczności stosowania art. 5, art. 12 – 22 oraz art. 34 RODO, które dotyczą naszych podstawowych praw w zakresie ochrony danych osobowych - od zasad przetwarzania danych poczynając, poprzez dopełnianie obowiązku informacyjnego przy zbieraniu danych, prawo dostępu do danych, prawo do sprostowania danych, prawo do bycia zapomnianym czy prawo do ograniczenia przetwarzania danych. Dotyczy to także obowiązku informowania nas o przypadku naruszenia ochrony danych osobowych. Podczas gdy określoną w RODO zasadą ma być informowanie nas bez zbędnej zwłoki o każdym naruszeniu ochrony naszych danych osobowych, jeżeli może to powodować wysokie ryzyko naruszenia naszych praw lub wolności, to polski projektodawca w wielu przypadkach proponuje wyłączenie tej zasady.

- Proszę podać przykłady.
- Ministerstwo Cyfryzacji proponuje na przykład, by sektor statystyki publicznej nie musiał stosować art. 5 ust. 2 rozporządzenia, w przypadku, gdyby spowodowało to nadmierny koszt po stronie statystyki publicznej.

- Co to znaczy w praktyce?
- To znaczy, że służby statystyki publicznej, gdyby mogło to spowodować po ich stronie nadmierny koszt, nie musiałyby stosować zasady rozliczalności, która jest fundamentalna dla unijnej reformy ochrony danych. Taka konstrukcja przepisu mającego wprowadzać w prawie polskim wyjątek od zasad przetwarzania danych osobowych przewidzianych w unijnym rozporządzeniu nie może zyskać akceptacji GIODO, bowiem brak jest w nim wskazania, która z wartości wymienionych w art. 23 ust. 1 rozporządzenia przemawia za jego wprowadzeniem i – co więcej – jaki miałby być jego zakres. Ponadto nie wiadomo, kto będzie oceniał, jaki koszt jest nadmierny, a jaki nie. Ustawodawca na to pytanie nie odpowiada, nie wskazuje żadnych kryteriów, na podstawie których miałaby zapadać decyzja w tym zakresie. W praktyce to organ statystyczny na zasadzie uznaniowości będzie decydował, czy przepis stosować.

- Jak dane osób mogą być zagrożone?
- Dane będą przetwarzane, a więc zbierane, wykorzystywane czy udostępniane, bez naszej wiedzy i zgody.
Inne istotne zagrożenie dla naszych danych rodzi np. propozycja wyłączenia stosowania art. 34 RODO przez sektor bankowy, gdyby mogło to spowodować naruszenie stabilności funkcjonowania sektora bankowego. Wprowadzenie tego przepisu oznaczałoby, że banki w przypadku wystąpienia incydentu z zakresu ochrony danych osobowych, nie musiałyby o tym

fakcie informować osób, których dane dotyczą, o ile ich zdaniem, takie zawiadomienie może spowodować naruszenie stabilności funkcjonowania sektora bankowego.

- Jakie są skutki nie poinformowania klientów banków?
- Przede wszystkim nie wiedzą oni, co się dzieje z ich danymi powierzonymi bankowi. Nie mają świadomości, że np. wyciekły, a przecież takie sytuacje, co potwierdza niedawny wyciek danych z czterech banków w Polsce, się zdarzają i z pewnością będą się zdarzały. Tymczasem bez szybkiej informacji o tym incydencie, klienci nie mogą podjąć żadnych środków zaradczych, by zminimalizować możliwe przykre konsekwencje wycieku danych, zadbać o bezpieczeństwo swoich środków finansowych. W naszej opinii, takie generalne wyłączenia są niedopuszczalne.
Warto jednocześnie podkreślić, że państwo członkowskie - zgodnie z art. 23 RODO - może aktem prawnym ograniczyć zakres wskazanych wyżej praw i obowiązków, ale ograniczenie to nie może naruszać podstawowych praw i wolności. Ponadto musi być środkiem proporcjonalnym i niezbędnym, służącym ważnym, wskazanym w tym przepisie celom, takim jak np. bezpieczeństwo narodowe czy publiczne, zapobieganie przestępczości albo ściganie przestępstw. Jeśli już w prawie krajowym wprowadza się ograniczenie, to w odpowiednim przepisie trzeba określić m.in. cele przetwarzania, kategorie danych, zakres wprowadzonych ograniczeń, zabezpieczenia zapobiegające nadużyciom lub niezgodnemu z prawem dostępowi bądź przekazywaniu, zasady przechowywania itd. Czyli RODO dopuszcza wprowadzanie ograniczeń, jeśli spełnione są warunki wskazane w jego art. 23. Jednak podkreślić należy, że artykuł ten mówi o ograniczeniach, a nie o wyłączeniach.
Według mnie, rozwiązania zaproponowane przez Ministerstwo Cyfryzacji są niezgodne z rozporządzeniem i wypaczają sens reformy. Mamy chronić dane osobowe, a nie wyłączać tę ochronę. Rozumiem, że należy mieć na względzie rozwiązania probiznesowe, ale każde wyłączenie stosowania RODO powinno wskazywać wartość, która uzasadnia takie ograniczenie podstawowych praw obywateli, jakimi są prawo do prywatności i ochrony danych osobowych. Zresztą, wydaje się, że RODO zapewnia właściwy balans pomiędzy prawami przedsiębiorców a prawami podmiotów danych, a proponowane przez Ministerstwo Cyfryzacji przepisy tę równowagę naruszają - i to na niekorzyść obywateli. Na to mojej zgody nie będzie.

- Jak może dotknąć to przedsiębiorców?
- Uważam, że wyłączenia ograniczające prawa każdego z nas w dłuższej perspektywie wcale nie ułatwią życia przedsiębiorcom, którzy poprzez te rozwiązania mogą stracić zaufanie swoich klientów.

- Największe zainteresowanie biznesu budzą dwie kwestie: sposoby certyfikacji i monitoring wizyjny. Czy RODO określiło zasady monitoringu?
- Monitoring wizyjny nie został w RODO uregulowany w sposób szczególny, więc podlega jego przepisom na takich samych zasadach, jak inne sposoby przetwarzania danych. W projekcie Ministerstwa Cyfryzacji przewidziano np. stosowanie monitoringu przez pracodawców, wprowadzając odpowiednie regulacje w Kodeksie pracy. Naszym zdaniem, jeśli te przepisy miałyby zacząć obowiązywać, to przynajmniej należałoby doprecyzować, w jakich pomieszczeniach w zakładzie pracy nie jest dopuszczalne montowanie kamer. Nie jest ponadto jasne, w jaki sposób miałaby być weryfikowana kwestia, czy monitoring wizyjny nie stanowi środka kontroli wykonywania przez pracownika zadań – zwłaszcza w sytuacji, gdy wideonadzór ma na celu zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, cel ten jest bowiem związany w sposób bezpośredni z właściwą realizacją przez pracownika jego obowiązków. Nasze zastrzeżenia budzi też okres

retencji danych oraz sposób dopełniania obowiązku informacyjnego o wprowadzeniu monitoringu. Natomiast nadal aktualny pozostaje podnoszony przez GIODO od lat postulat, aby kwestie monitorowania przestrzeni przy pomocy kamer zostały kompleksowo uregulowane w odrębnym akcie rangi ustawowej. .

- Jeśli przedsiębiorca sam by chciał ustalić reguły monitoringu i siebie w firmie?
- Musi wtedy przeanalizować przepisy RODO i zastanowić się, czy rozwiązania, które zamierza wdrożyć, są z nimi zgodne, a więc m.in., czy ma podstawy prawne do takiego przetwarzania danych osobowych, czy zakładanego celu nie można osiągnąć przy pomocy środków mniej ingerujących w prywatność. Musiałby przeanalizować, jak długo ma prawo przechowywać nagrania, jak powinien je zabezpieczyć itd.

- Polski projekt ustawy idzie w tym kierunku, że ten kto przyznaje certyfikat może nałożyć jednocześnie karę na przedsiębiorcę. Czy Pani się zgadza z taką konstrukcją, kto certyfikaty powinien wydawać?
- Ministerstwo Cyfryzacji początkowo proponowało, że organ nadzorczy będzie jedynie akredytował podmioty certyfikujące. Najnowsza propozycja resortu zakłada, że organ będzie jedynym uprawnionym do udzielania certyfikatów. Ja od początku dyskusji na te tematy, bazując na dotychczasowym 20-letnim doświadczeniu urzędu, a także doświadczeniach moich odpowiedników z innych państw członkowskich UE, proponowałam przyjęcie modelu hybrydowego, uznając go za najwłaściwszy i najskuteczniejszy.
W mojej ocenie, krąg podmiotów przyznających certyfikaty powinien być jak najszerszy. W różnych państwach europejskich to właśnie organy ochrony danych osobowych prowadzą programy certyfikacyjne, co w żaden sposób nie ogranicza funkcjonowania rynku podmiotów certyfikujących, lecz raczej ten rynek wzmacnia i stymuluje. Tym bardziej że teraz już nie będziemy mogli mówić jedynie o krajowym rynku certyfikatów w zakresie ochrony danych osobowych, lecz raczej o rynku europejskim, i to tam będzie się rozgrywała konkurencja pomiędzy dostępnymi mechanizmami certyfikacyjnymi. Tymczasem proponowane przez Ministerstwo Cyfryzacji rozwiązanie może skutkować tym, że w Polsce rynek certyfikacji w ogóle się nie rozwinie. Także dlatego, że z pewnością polskim administratorom będą oferowane certyfikaty przez podmioty certyfikujące z innych państw członkowskich UE.
Opiniując tę wersję projektu ustawy o ochronie danych osobowych, w którym zaproponowano, aby krajowy organ nadzorczy udzielał akredytacji podmiotom certyfikującym, wskazywałam, że rozwiązanie takie jest możliwe i korzystne z punktu widzenia prestiżu i pozycji Biura. Podnosiłam jednak możliwość wykonywania tego zadania przez istniejącą krajową jednostkę akredytującą - Polskie Centrum Akredytacji. To ważne, by w procesie akredytacji podmiotów certyfikujących spełnić rygorystyczne procedury dotyczące zapewnienia transparentności i niezależności. Poszczególne etapy procesu, takie jak weryfikacja warunków, audyt akredytacyjny, ocena wyników i ich zatwierdzenie, powinny być realizowane przez różne osoby.
Ponadto chciałabym podnieść jeszcze jeden aspekt tego zagadnienia – termin na dokonanie akredytacji. Moim zdaniem, zaproponowany termin 3 miesięcy na przeprowadzenie certyfikacji wydaje się zbyt krótki, szczególnie wobec wielu skomplikowanych czynności, jakie należy w toku tej procedury podjąć. W przypadku podmiotów o złożonej strukturze, dokonanie akredytacji w 3-miesięcznym terminie może być niewykonalne. Tym bardziej że termin na dokonanie certyfikacji powinien być uzależniony od tego, co będzie podlegało certyfikacji – to bowiem, czy przyznajemy znaki jakości stronom internetowym, czy też certyfikujemy zaawansowane środki bezpieczeństwa wpływa na złożoność tego procesu.

- Nie każdy musi mieć certyfikat.
- Tak, ale zgłaszają się różne podmioty, aby uzyskać certyfikację i dlatego należałoby wydłużyć ten okres przynajmniej do pół roku.

- Czy marketingowcy będą mieli więcej problemów od 25 maja 2018 r., gdy wejdzie w życie rozporządzenie? Chodzi o wyraźne zgody.
- Kwestią nie budzącą wątpliwości jest to, że od 25 maja 2018 r. wszyscy administratorzy danych będą musieli wykazać zgodność wszystkich procesów przetwarzania danych z ogólnym rozporządzeniem o ochronie danych. Jeśli więc dane przetwarzane są obecnie na podstawie zgody osoby, której dane dotyczą, zgoda ta od 25 maja 2018 r. będzie musiała odpowiadać warunkom rozporządzenia. Jeśli faktycznie tak będzie, to – jak stanowi motyw 171 RODO – nie będzie potrzeby ponownego jej wyrażania przez podmiot danych. W tym kontekście pojawia się jednak pewien problem. Dotyczy on obowiązku uprzedniego poinformowania podmiotu danych o możliwości wycofania zgody (vide art. 7 ust. 3 RODO). Choć przepisy ustawy o ochronie danych osobowych przewidują obecnie możliwość odwołania zgody w każdym czasie (o czym wprost stanowi jej art. 7 pkt 5), to jednak nie wskazano w nich wprost, że o takiej możliwości należy poinformować osoby, których dane dotyczą. Co więcej, RODO wymaga, aby odwołanie zgody było tak samo łatwe jak jej udzielenie.

- Czy kwestia tego, czy trzeba będzie ponownie pozyskiwać zgodę wobec braku uprzedniego poinformowania podmiotu danych o możliwości jej wycofania, jest rozważana na forum Grupy Roboczej Art. 29 - organu doradczego Komisji Europejskiej w zakresie ochrony danych osobowych?

- Być może ta kwestia zostanie jednolicie rozwiązana na poziomie wszystkich państw członkowskich UE, choć ze względu na dotychczasowe różnice w prawodawstwie i podejściach krajowych może do tego nie dojść. Jeśli tak będzie, GIODO na pewno przedstawi własne zalecane podejście do tego zagadnienia.
Rozważając kwestię zgody, warto zwrócić uwagę na jeszcze jeden aspekt tej sprawy i zaznaczyć, że RODO wymaga, aby język zapytania o zgodę był prosty i zrozumiały dla osoby, która ma zgody udzielić, a same komunikaty łatwo dostępne. Należy więc np. unikać zawiłych terminów i nie umieszczać objaśnień drobnym druczkiem.
To jest niezmiernie istotne przy wyrażaniu zgód przez dzieci, które rozporządzenie zaleca zresztą traktować w sposób szczególny. RODO przewiduje, że dziecko powyżej 16 roku życia może samodzielnie wyrażać zgodę na przetwarzanie jego danych osobowych na potrzeby korzystania z usług społeczeństwa informacyjnego, czyli portali społecznościowych czy gier on-line. Państwa członkowskie w swoich ustawodawstwach krajowych mogą przyjąć niższą granicę wiekową, ale nie niższą niż lat 13, od której bez udziału rodziców dziecko samo może w takich sytuacjach wyrazić zgodę na przetwarzanie jego danych. I tak też przyjął nasz ustawodawca, uzasadniając to tym, że lat 13 to wiek, w którym zgodnie z Kodeksem cywilnym uzyskuje się ograniczoną zdolność do czynności prawnych. Ale jest to ograniczona zdolność do czynności prawnych w drobnych sprawach życia codziennego, tak, aby dziecko mogło kupić sobie bilet na autobus czy bułkę. Sprawa już nie jest taka prosta chociażby w przypadku zatrudniania dzieci. Zgodnie z Kodeksem pracy, wykonywanie pracy lub innych zajęć zarobkowych przez dziecko do ukończenia przez nie 16 roku życia jest dozwolone wyłącznie na rzecz podmiotu prowadzącego działalność kulturalną, artystyczną, sportową lub reklamową. Jednocześnie wymaga to m.in. zgody rodzica i zezwolenia właściwego inspektora pracy oraz opinii dyrektora szkoły.
Wybory dziecka w internecie są bardziej skomplikowane, to nie tylko gry on-line, ale też np.

ściąganie darmowych aplikacji, za które jednak „płacimy” naszą prywatnością, naszymi danymi osobowymi.

- Czyli 13-latek nie może podjąć świadomej decyzji w zakresie wykorzystania internetu?

- Tak, istnieje taka obawa i potwierdzają to prowadzone przez nas konsultacje m.in. z Rzecznikiem Praw Dziecka czy MEN. Wskazują na to również wyniki ankiety przeprowadzonej w szkołach, które w ubiegłym roku uczestniczyły w programie edukacyjnym GIODO „Twoje dane – Twoja sprawa”. Aż 89 proc. pedagogów uznało, że 13 lat to zbyt mało, by dziecko mogło samodzielnie wyrazić zgodę na przetwarzanie danych osobowych w związku z korzystaniem usług cyfrowych. Trzeba pamiętać, że choć młode pokolenie jest pokoleniem informacyjnym, idealnie poruszającym się w nowościach technologicznych, to jednocześnie nie ma wystarczającej wiedzy z dziedziny praw i obowiązków obywatelskich. Ma też bardzo niską świadomość co do konsekwencji udostępniania swoich danych osobowych oraz wykorzystywania i przetwarzania danych osobowych kolegów i koleżanek. Trudno byłoby więc uznać, że zgoda udzielana przez dzieci jest wyrażana w sposób świadomy, co jest jednym z warunków uznania jej za prawidłową podstawę uprawniającą do przetwarzania danych.
W moim przekonaniu, decyzja o wyznaczeniu wieku, od którego dzieci, korzystając z usług cyfrowych, będą mogły same wyrażać zgodę na przetwarzanie swoich danych osobowych, wymaga głębokiego namysłu i uwzględnienia zarówno psychologicznych oraz pedagogicznych, jak i prawnych aspektów tego problemu.

- Będą też problemy ze sprawdzeniem, czy rodzic wyraża zgodę na przetwarzanie, bo jak to sprawdzić?

- To kolejna problematyczna sprawa. Ale proszę też wziąć pod uwagę jeszcze jeden aspekt tego zagadnienia, a mianowicie to, że w razie naruszenia dziecko nie może złożyć skargi do Generalnego Inspektora Ochrony Danych Osobowych. Tak czy inaczej, zawsze rodzice będą odpowiadać i płacić za decyzje i działania dziecka w sieci. To może być duże pole do nadużyć.

- Polskie Przepisy wprowadzające ustawę o ochronie danych osobowych, wprowadzają kilka nieuzasadnionych zmian obniżających ochronę osób, których dane dotyczą. Jakie są to obszary?

- Tych obszarów jest wiele, a o części z nich już mówiłam. Niemniej niepokoi mnie jeszcze skala wykorzystywania numeru PESEL. W świetle przepisów RODO powinien on być poddany szczególnej ochronie, a polski projektodawca zdaje się tę kwestię bagatelizować czy pomijać.
Mam też poważne wątpliwości co do pozyskiwania danych biometrycznych pracowników. Ministerstwo Cyfryzacji proponuje zmianę art. 22 ze znaczkiem 1 Kodeksu pracy, wprowadzając rozwiązanie, które zezwala pracodawcy na gromadzenia danych biometrycznych, czyli np. odcisków palców, obrazu siatkówki oka itd.

- Gdzie Pani minister widzi zagrożenie?

- Zgodnie z utrwalonym poglądem wyrażanym zarówno przez GIODO, jak i NSA – rzeczywista dobrowolność wyrażania zgody na przetwarzanie danych w stosunkach pracy jest wyjątkiem. Wynika to z charakteru prawnego stosunku pracy i podporządkowania, zależności pracownika od pracodawcy. Tu nie ma równowagi stron. W sytuacjach szczególnych, jak np. kontrola wejść do skarbca w banku czy do magazynu z cennym kruszcem lub drogim sprzętem, zastosowanie biometrii może być uzasadnione. Ale czy pobieranie danych

biometrycznych, które zgodnie z RODO należą do danych szczególnej kategorii i powinny być szczególnie chronione, w każdej sytuacji pracowniczej jest uzasadnione? Wydaje się, że przy projektowaniu przepisów w tym zakresie zapomniano o jednej z podstawowych zasad – minimalizacji danych. Zgodnie z nią, jeśli da się osiągnąć ten sam cel, mniej ingerując w dane osobowe i prywatność pracownika, to ten cel powinniśmy osiągnąć przy użyciu takich właśnie mniej inwazyjnych środków. I dlatego np. ewidencja czasu pracy z wykorzystaniem biometrii nie powinna być dozwolona. Ponadto wszystkie umowy cywilno-prawne z pracownikami nie będą podlegać tym regułom, bo nie są objęte przepisami Kodeksu pracy. Co więcej, dane biometryczne są nie do odtworzenia, co rodzi określone zagrożenia, jeśli zaginą lub wyciekną. Nie można zastrzec skanu siatkówki oka, gdy taki skan zostanie zgubiony lub wykradziony. Inna osoba może się poddać weryfikacji np. w banku, gdy będzie dysponować skradzionym skanem. A co więcej, nie każdy człowiek posiada np. odciski palców. Mam wątpliwości, czy powszechne dopuszczenie biometrii będzie wiązało się z ochroną danych. Dlaczego wprowadzać tak radyklane metody weryfikacji tożsamości, skoro można to samo osiągnąć innymi, bardziej adekwatnymi środkami, mniej ingerującymi w naszą prywatność? Obawiam się, że również pracodawcom wdrożenie takich rozwiązań może przysporzyć więcej kłopotów niż pożytku.

- **Ministerstwo Cyfryzacji twierdzi, że nie ma konfliktu interesów między mianowaniem wiceprezesów nowego urzędu kontroli danych przez ministrów spraw wewnętrznych i cyfryzacji. Chodzi o sprawny przepływ informacji. Czy Pani się z tym zgadza?**
- Nie. Gdyby przyjąć tę argumentację można by zapytać, dlaczego środowiska biznesowe nie miałyby wskazywać wiceprezesa – z tym sektorem GIODO również powinien współpracować.
Podejście przyjęte przez Ministerstwo Cyfryzacji świadczy o niezrozumieniu istoty niezależności organu ochrony danych osobowych. Współpraca, oczywiście, jest konieczna i od zawsze współpracujemy ze wszystkimi instytucjami. Jednocześnie jednak mamy za zadanie kontrolować przestrzeganie prawa przy przetwarzaniu danych osobowych zarówno w sektorze publicznym, jak i prywatnym. Rodzi się więc pytanie, czy jest to możliwe w sytuacji, gdy zastępcy prezesa UODO są wskazywani przez dwa resorty i powoływani przez premiera. Obecny system powoływania i gwarancje niezależności organu spełniały bardzo wysokie standardy europejskie, na co wskazywała również doktryna. Nie widzę powodu, dla którego miałoby się to zmieniać, na pewno nie wymaga tego rozporządzenie. Najważniejsze jest to, żeby urząd mógł się cieszyć niezależnością, bo tylko wtedy będzie mógł właściwie wykonywać swoje zadania, w tym kontrolne wobec administracji rządowej. Nie może też być poddany żadnym politycznym wpływom. Tymczasem stwarzamy tutaj zupełnie dysfunkcyjny model zarządzania organem. Rodzi się, niestety, skojarzenie o upolitycznienie urzędu.

Rozmawiała: Katarzyna Żaczkiewicz-Zborska

Katarzyna Żaczkiewicz-Zborska 09.11.17