Sprawozdanie krajowe polskiego organu nadzorczego

Część I – statystyka

Polski organ nadzorczy, biorąc udział w CEF DPO, zdecydował się nie rozsyłać wspólnego formularza. Decyzja ta wynikała z faktu, że polski organ, jeszcze przed rozpoczęciem CEF DPO, rozesłał do krajowych administratorów i podmiotów przetwarzających (zarówno z sektora publicznego, jak i prywatnego) 27 przygotowanych przez siebie pytań, które dotyczyły kluczowych obowiązków administratorów zakresie zapewnienia prawidłowego wykonywania funkcji IOD (art. 37-39 RODO). Pytania te są dostępne pod adresem: https://archiwum.uodo.gov.pl/pl/138/2336.

Podmioty, do których skierowano pytania, zostały zobowiązane, zgodnie z zasadą rozliczalności, do przedstawienia szczegółowych wyjaśnień dotyczących rozwiązań przyjętych w odniesieniu do każdego z ich obowiązków wynikających z art. 37-39 RODO, wraz z odpowiednimi dowodami potwierdzającymi złożone wyjaśnienia. Postępowania wszczęte w związku z otrzymanymi odpowiedziami w tym zakresie są nadal w toku.

Żeby nie wprowadzać administratorów w błąd co do celu podjętych wcześniej działań i przesłanych pytań oraz ze względu na trwające postępowania krajowe wszczęte w związku z otrzymanymi odpowiedziami, polski organ nadzorczy nie zaangażował się w dystrybucję formularza opracowanego na potrzeby „akcji CEF 2023 dotyczącej wyznaczania i roli inspektorów ochrony danych".

W związku z powyższym załącznik "statystyki" nie zawiera danych dotyczących PL SA.

Część II – kwestie merytoryczne

W kilku podmiotach UODO zidentyfikował problem świadczenia przez firmy zatrudniające inspektorów ochrony danych usług outsourcingu funkcji IOD i jednocześnie usług polegających na wykonywaniu za administratora tzw. wdrożenia RODO oraz innych usług związanych z analizą i oceną ryzyka, obsługą żądań i roszczeń podmiotów danych, szeroko rozumianym bezpieczeństwem informacji. Tym samym ta sama osoba decydowała o zasadach przetwarzania danych osobowych, sposobie wykonywania obowiązków administratora, identyfikowaniu i ocenie ryzyka związanego z przetwarzaniem oraz zabezpieczaniem danych osobowych, a następnie - w ramach pełnienia funkcji IOD - dokonywała oceny prawidłowości podjętych przez siebie decyzji i rozwiązań. Prowadziło to do sytuacji, w której IOD monitorował własną działalność, a więc do konfliktu interesów, czego wprost zakazuje art. 38 ust. 6 RODO.

Zgodnie z art. 38 ust. 6 RODO IOD może wykonywać inne zadania i obowiązki, o ile administrator lub podmiot przetwarzający zapewni, aby te zadania i obowiązki nie powodowały konfliktu interesów. Ze względu na charakter zadań IOD skupiających się na doradzaniu oraz monitorowaniu działalności administratora pod kątem zgodności operacji przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz wymóg sprawowania tej funkcji w sposób niezależny, administrator nie powinien nakładać na IOD zadań, które zgodnie z przepisami RODO należą do administratora. Przyjęcie odmiennego założenia, w którym IOD byłby odpowiedzialny za wykonanie określonego zadania administratora, np. zgłaszanie naruszeń, a jednocześnie miałby monitorować zgodność wykonywania tego zadania z przepisami o ochronie danych osobowych, do czego zobowiązuje go unormowanie zawarte w art. 39 ust. 1 lit. b RODO, doprowadziłoby do sytuacji, w której IOD sprawowałby *de facto* nadzór nad własną działalnością, a więc do konfliktu interesów.

Konflikt interesów następuje m.in. wtedy, gdy nie można pogodzić prawidłowego wykonywania zadań inspektora, przypisanych mu w art. 38 ust. 4 oraz art. 39 RODO, z realizacją innych zadań, gdyż pomiędzy zadaniami występuje sprzeczność, uniemożliwiająca odpowiednią ich realizację. W przypadku inspektora sprzeczność taka może wynikać z występowania przez niego jednocześnie w dwóch rolach lub podejmowania przez niego działań lub decyzji, które następnie muszą podlegać jego ocenie zgodnie z art. 39 ust. 1 lit. b RODO.

IOD, którego głównym zadaniem jest zapewnienie właściwego przestrzegania przepisów o ochronie danych osobowych, musi mieć dla tego celu zagwarantowane odpowiednie warunki funkcjonowania, a więc takie, które pozwolą mu na efektywną, niezależną oraz prawidłową realizację obowiązków wynikających z przepisów prawa, co wynika z art. 38 ust. 2 i 3 RODO. Nakładanie na IOD obowiązków prowadzących do powstania konfliktu interesów stawia pod znakiem zapytania nie tylko możliwość efektywnego wypełniania przez niego zadań, do realizacji których zobowiązuje go dyspozycja normy art. 39 RODO, ale godzi w same fundamenty instytucji IOD opartej w pierwszym rzędzie na niezależności funkcjonowania.

Ponadto w kilku postępowaniach stwierdzono następujące problemy: brak procedur zapewniających unikanie konfliktu interesów, zawieranie z podmiotami świadczącymi usługi zewnętrznego IOD równocześnie umowy powierzenia przetwarzania danych, co stoi w sprzeczności z przewidzianym w art 38 ust. 3 RODO obowiązkiem zapewnienia przez administratrora, aby inspektor nie otrzymywał instrukcji dotyczących swoich zadań, reprezentowanie administratora przez IOD w charakterze pełnomocnika, niepodleganie przez IOD najwyższemu kierownictwu administratora, brak zapewnienia mechanizmów kontroli nad prawidłowym i planowym wykonywaniem zadań przez IOD, brak wykazania, że administrator wspiera IOD i zapewnia IOD odpowiednie zasoby, w tym na podnoszenie poziomu wiedzy fachowej.

Część III – działania organu nadzorczego

1. Czy opublikowano ogólne wytyczne (np. przewodniki, wytyczne itp.) dotyczące inspektorów ochrony danych (w tym przed rozpoczęciem skoordynowanego działania)?
Jeżeli tak, proszę podać datę, link do wytycznych i krótki opis wytycznych

Takie wytyczne i podpowiedzi były przez UODO publikowane zarówno przed rozpoczęciem stosowania RODO, jak i po 25.05.2018 r. Przed wejściem w życie przepisów RODO prowadzony był portal informacyjny ABI-informator, w którym oprócz wyjaśnień dotyczących funkcjonowania i statusu ABI (poprzednika inspektora ochrony danych) zamieszczane były też wskazówki i odpowiedzi na kierowane do UODO pytania dotyczące inspektorów ochrony danych i RODO. Od 25.05.2018 r. na stronie internetowej UODO prowadzona jest zakładka „Inspektor Ochrony Danych" podzielona na następujące sekcje:

- Wyznaczenie i status IOD (poprzednia strona UODO - https://archiwum.uodo.gov.pl/p/wyznaczenie-i-status-iod; obecna strona UODO - https://uodo.gov.pl/pl/495,).
- Zawiadomienia Prezesa UODO związane z IOD – (poprzednia strona UODO - https://archiwum.uodo.gov.pl/pl/p/zawiadomienia-prezesa-uodo-zwiazane-z-iod)
- Zadania IOD – (poprzednia strona UODO - https://archiwum.uodo.gov.pl/pl/p/zadania-iod).

W zakładce o nazwie „Inspektor Ochrony Danych" publikowane były odpowiedzi na pytania, jakie przedstawiali w tym zakresie inspektorzy oraz administratorzy. Zamieszczane wskazówki miały na celu ułatwienie im wywiązywania się z nałożonych przepisami RODO obowiązków i zadań oraz wypracowanie odpowiednich, dostosowanych do ich organizacji rozwiązań. Poruszane były w niej zagadnienia dotyczące wyznaczenia i statusu inspektora ochrony danych (w tym m.in. szczegółowe wskazówki dotyczące kwalifikacji IOD, konfliktu interesów, oceny dopuszczalności łączenia funkcji IOD z różnymi innymi stanowiskami, wyjaśnienia dotyczące braku możliwości zawierania z zewnętrznym IOD umowy powierzenia, a także zapewnienia inspektorowi określonych zasobów) oraz o zadaniach inspektorów ochrony danych (w szczególności jakie zadania są przypisane IOD, a które zadania ma obowiązek wykonywać administrator i nie powinien tych zadań przerzucać na IOD). W zakładce zamieszczone były też szczegółowe instrukcje nt. prawidłowego powiadomienia organu nadzorczego o wyznaczeniu inspektora ochrony danych oraz publikowania jego danych przez adminsitratora lub podmiot przetwarzający na ich stronie internetowej do wiadomości osób, których dane dotyczą). W sekcji „Zadania IOD" zamieszczane były wskazówki, jak rozstrzygać szczegółowe problemy, jakie napotykali inspektorzy w swojej praktyce w odniesieniu do zastowania właściwych przesłanek przetwarzania danych osobowych, pojęć „administrator",

„współadministrator”, „podmiot przetwarzający”, obowiązków administratora lub podmiotu przetwarzającego oraz odpowiedzi na pytania dot. udostępniania danych osobowych.

Organ podkreślał w swoich materiałach, iż decyzja w zakresie wyboru odpowiedniej osoby do pełnienia funkcji inspektora musi być podejmowana z pełną świadomością ciążącej na administratorze odpowiedzialności za prawidłowe przestrzeganie przepisów prawa. Administrator przed wyznaczeniem konkretnej osoby do pełnienia funkcji IOD musi brać pod uwagę wiele czynników. Ocena przeprowadzona przez administratora powinna uwzględniać: efektywną dostępność inspektora, możliwość uzyskania przez niego szczegółowej wiedzy na temat funkcjonowania podmiotu, dysponowanie przez niego ilością czasu odpowiednią do zakresu zadań i specyfiki procesów przetwarzania danych, wielkość i strukturę organizacyjną jednostki będącej administratorem oraz konieczność unikania konfliktu interesów. W naszym zamierzeniu przekazanie takich wskazówek było ważne, ponieważ zapewnienie IOD właściwego statusu przekłada się na prawidłowe wykonywanie przez niego zadań.

Polski organ nadzorczy wielokrotnie odnosił się do kwestii konfliktu interesów oraz dopuszczalności łączenia funkcji IOD z różnymi innymi stanowiskami, tj. np. pełnomocnika ds. informacji niejawnych, kierownika komórki organizacyjnej, administratora systemu informatycznego, czy pracą w roli adwokata i radcy prawnego. W każdej ze swoich rekomendacji dotyczących statusu IOD organ podkreślał, iż ocena, czy w przypadku konkretnej osoby i wykonywanych przez nią zadań nie występuje konflikt interesów, powinna być dokonywana indywidualnie z uwzględnieniem konkretnych okoliczności. Oznacza to, że możliwość zaistnienia konfliktu powinna być stale monitorowana, ponieważ przyczyny takiego konfliktu mogą wystąpić również w późniejszym czasie, po rozpoczęciu pełnienia funkcji przez IOD. Administrator powinien przy tym uwzględnić m.in. następujące kryteria: organizacyjne (IOD powinien podlegać bezpośrednio najwyższemu kierownictwu jednostki organizacyjnej), merytoryczne (inne obowiązki nie powinny negatywnie wpływać na niezależne wykonywanie zadań IOD), czasowe (IOD powinien dysponować czasem wystarczającym do wykonywania swoich zadań, przy uwzględnieniu m.in. liczby obowiązków czy stopnia ich skomplikowania).

W reakcji na pytania od inspektorów polski organ nadzorczy odniósł się do kwestii obowiązku zapewnienia odpowiednich zasobów, o którym mowa w art. 38 ust. 2 RODO. Ten obowiązek administratora ściśle łączy się z planowaniem pracy przez inspektora i przedstawianiem tego planu administratorowi (podmiotowi przetwarzającemu). Stworzenie przez IOD planu działania ułatwia jak najlepsze i realne wykorzystanie zasobów, którymi dysponuje jako IOD. Tworzenie planu pomaga ustalić, czy zasoby te są wystarczające, a także, czy we wszystkich monitorowanych obszarach IOD ma zapewnione przez administratora współdziałanie ze strony osób przetwarzających dane osobowe i posiadających wiedzę na temat tego przetwarzania. Istotne jest, aby w wewnętrznych procedurach administratora

znalazły się odpowiednie regulacje w tym zakresie. Taki plan powinien uwzględniać wiele czynników zależnych od specyfiki danego administratora i prowadzonych przez niego procesów (czynności) przetwarzania danych. Konieczne jest jego dostosowanie do przeprowadzonej w organizacji oceny ryzyka (do tego zobowiązuje IOD art. 39 ust. 2 RODO) i przypisanie wyższego priorytetu obszarom, które mają szczególne znaczenie dla systemu ochrony danych u konkretnego administratora (https://archiwum.uodo.gov.pl/pl/225/1870). Warto, aby kwestie zapewniania odpowiednich zasobów oraz planu pracy inspektora były odzwierciedlone w regulacjach wewnętrznych administratora (podmiotu przetwarzającego).

Ponadto wiele informacji, w tym również w zakresie prawidłowego wykonywania przez IOD zadań, można znaleźć w Newsletterze UODO dla Inspektorów Ochrony Danych wydawanym cyklicznie od 2019. Archiwum „Newsletter UODO dla Inspektorów Ochrony Danych" za okres od kwietnia 2019 r. do listopada 2022 r. dostępne jest pod następującym linkiem: https://archiwum.uodo.gov.pl/p/archiwum-newslettera-dla-iod. Kolejne numery „Newsletter UODO dla Inspektorów Ochrony Danych" (od marca 2023 r. funkcjonującego pod nazwą „Biuletyn UODO") można znaleźć pod linkiem: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.

Od 2016 r. do 2019 r. polski organ nadzorczy prowadził cykl nieodpłatnych szkoleń dla inspektorów ochrony danych (IOD) z wybranych sektorów (m.in. oświatowego, medycznego, sądownictwa, fundacji i stowarzyszeń oraz ośrodków pomocy społecznej). Sektorowe szkolenia koncentrowały się na nowych unijnych przepisach o ochronie danych osobowych oraz przepisach krajowych, mających zastosowanie do przetwarzania danych w określonej dziedzinie działalności. Szkolenia te nie tylko podniosły poziom wiedzy inspektorów ochrony danych obsługujących daną branżę, ale stanowiły także okazję do wymiany doświadczeń, rozwiązań i dobrych praktyk pomiędzy uczestnikami tych spotkań. Organ nadzorczy zrealizował również cykl szkoleń dotyczących wybranych zasad i obowiązków wynikających z przepisów o ochronie danych osobowych, np. zasada przejrzystości i spełnianie obowiązków informacyjnych (art. 13, 14 RODO), przekazywanie danych osobowych do państw trzecich (art. 44 – 49 RODO), zgłaszanie naruszenia ochrony danych osobowych (art. 33 RODO), przeprowadzanie oceny skutków dla ochrony danych osobowych (art. 35 RODO). Odrębne szkolenie dla inspektorów poświęcone było przepisom przyjętym w Polsce na podstawie dyrektywy 2016/680.

Od lutego 2019 r UODO uruchomił infolinię dla IOD, która w marcu 2020 r. została przekształcona w infolinię dla wszystkich interesantów, w tym IOD.

2. **Czy przed rozpoczęciem skoordynowanego działania podjęli Państwo działania (tj. dochodzenia, spotkania, uprzednie konsultacje, postępowania) wobec którejkolwiek z organizacji, dotyczące wyznaczenia, zadań lub roli inspektora ochrony danych? Proszę opisać podjęte przez Państwa działania**

i wyniki tych działań (np. pismo, zalecenia dla organizacji, ogólne wytyczne, środki naprawcze, takie jak nakazy, nakazy zaprzestania szkodliwych praktyk z karą przyrostową lub bez niej, administracyjne kary pieniężne).

Od początku stosowania przepisów RODO zarówno w ramach prowadzonych postępowań, jak i w reakcji na zgłaszane UODO przypadki nieprzestrzegania przepisów dotyczących inspektorów ochrony danych podejmowane były działania wynikające z uprawnień organu nadzorczego określonych w art. 58 RODO. Podczas czynności kontrolnych w podstawowym zakresie sprawdzane były kwestie przestrzegania przepisów dotyczących prawidłowego wyznaczenia i funkcjonowania inspektora. Sprawdzeniu podlegały m.in. kwestie związane z obowiązkiem wyznaczenia inspektora, zgłoszenia organowi nadzorczemu wyznaczenia lub odwołania inspektora, opublikowania imienia i nazwiska inspektora na stronie internetowej administratora, usytuowania inspektora w strukturze organizacji, włączania go w sprawy ochrony danych osobowych, a także ewentualnego występowania konfliktu interesów.

W większości sytuacji weryfikacja ta wypadała pozytywnie i nie dawała podstaw do zastosowania uprawnień naprawczych. Jedynie w kilku przypadkach UODO w toku czynności kontrolnych stwierdził nieprawidłowości w zakresie występowania konfliktu interesów, np. pełnienia funkcji IOD przez sekretarza gminy czy też niekonsultowania z inspektorem podejmowanych operacji przetwarzania danych osobowych.

Kilka przypadków naruszenia przepisów związanych z pełnieniem funkcji inspektora wymagało podjęcia przez organ nadzorczy działań naprawczych określonych w art. 58 ust. 2 RODO, w tym wydania nakazu wyznaczenia inspektora ochrony danych w spółdzielni mieszkaniowej, a także nałożenia administracyjnej kary pieniężnej w związku z wypełnianiem przez inspektora swoich zadań bez należytego uwzględnienia ryzyka związanego z operacjami przetwarzania oraz nieangażowania inspektora w prowadzone procesy przetwarzania.

Jeśli chodzi o nieprawidłowości zgłaszane przez inspektorów ochrony danych (a także czasem przez inne podmioty), to dotychczas nie było wiele takich sygnałów i dotyczyły one przede wszystkim:
- nieopublikowania na stronie internetowej administratora imienia i nazwiska inspektora,
- nieaktualizowania danych inspektora na stronie internetowej administratora,
- przyjęcia procedur obciążających inspektora obowiązkami powodującymi konflikt interesów,
- zapisania w regulaminie organizacyjnym, że IOD może być odwołany w każdym czasie,
- przyczyn odwołania inspektora,
- nieprawidłowego usytuowania IOD w strukturze organizacyjnej administratora - IOD nie podlegał bezpośrednio najwyższemu kierownictwu,

- niezapewnienia inspektorowi wystarczającej ilości czasu oraz innych zasobów niezbędnych do wykonywania jego zadań,
- niezapewnienia inspektorowi wsparcia finansowego, infrastrukturalnego oraz możliwości aktualizowania wiedzy,
- pomijania inspektora w sprawach dotyczących przetwarzania danych osobowych (w tym takich, w których administratorzy prosili o opinię UODO, nie zwracając się wcześniej o opinię do inspektora).

W każdej zgłaszanej przez inspektorów sytuacji UODO na podstawie art. 58 ust. 1 lit. a i e RODO wzywał administratorów do złożenia wyjaśnień dotyczących przyjętych przez nich rozwiązań w zakresie konkretnego obowiązku wynikającego z przepisów o ochronie danych osobowych wraz z przedstawieniem szczegółowych i popartych dowodami informacji na temat regulacji i praktyk przyjętych w celu prawidłowej realizacji tego obowiązku. We wszystkich tych przypadkach administratorzy wskazali, że podjęli działania w celu dostosowania swojej działalności do przepisów dotyczących inspektorów ochrony danych, przedstawiając zmienione, szczegółowe rozwiązania organizacyjne służące temu celowi. Jedynie w jednej sprawie została wydana decyzja, w której organ nadzorczy udzielił upomnienia, stwierdzając naruszenie przez jeden ze szpitali przepisu art. 38 ust. 6 RODO w zakresie, w jakim szpital zobowiązywał inspektora ochrony danych do nadawania personelowi upoważnień do przetwarzania danych.

3. **Jakie działania zamierzają Państwo podjąć w oparciu o ewentualne wyniki tego skoordynowanego działania? (np. pismo, zalecenia dla organizacji, ogólne wytyczne, środki naprawcze, takie jak nakazy, nakazy zaprzestania szkodliwych praktyk z karą przyrostową lub bez niej, administracyjne kary pieniężne). W miarę możliwości proszę wskazać harmonogram tych działań (również w przypadku, gdy formalne dochodzenia są nadal w toku).**

W związku ze stwierdzonymi naruszeniami przepisów RODO, przewiduje się wszczęcie postępowań administracyjnych oraz wydanie decyzji nakładających obowiązek dostosowania warunków działania IOD do wymogów RODO oraz nałożenie kar pieniężnych, w przypadkach gdy będą zachodziły przesłanki do zastosowania takiej sankcji.

Część IV – inne

1. Jakie jest Państwa ogólne wrażenie co do poziomu świadomości i zgodności z RODO działań tych organizacji, z którymi konsultowali się Państwo w sprawie wyznaczenia, zadań lub roli inspektora ochrony danych?

Zaobserwowano, że w niektórych przypadkach poziom świadomości jest niewystarczający, przy czym co do zasady podmioty mają świadomość i na ogół

przestrzegają najważniejszych norm wynikających z przepisów dotyczących wykonywania zadań przez IOD.

2. **Czy są jakieś inne problemy lub tematy, które chcieliby Państwo zasygnalizować?**

W wyniku działań UODO polegających na weryfikacji przestrzegania przepisów dotyczących IOD w kilku organizacjach zidentyfikowany został problem nakładania przez administratora na IOD zadania dotyczącego prowadzenia rejestru czynności przetwarzania, co powoduje konflit interesów, o którym mowa w art 38 ust. 6 RODO. IOD nie może bowiem podejmować działań lub decyzji, które następnie muszą podlegać jego ocenie zgodnie z art. 39 ust. 1 lit. b RODO. Z brzmienia art. 30 ust. 1 RODO wynika, że prowadzenie rejestru czynności przetwarzania należy do obowiązków administratora.

W ocenie UODO obecne brzmienie Wytycznych dotyczących inspektorów ochrony danych WP 243 rew.01 dopuszczające możliwość wykonywania przez IOD zadania administratora, jakim jest prowadzenie rejestru czynności przetwarzania, wymaga dostosowania do aktualnego stanu prawnego. Realizowanie tego zadania przez IOD prowadzi do powstania konfliktu interesów, którego występowania zakazuje w odniesieniu do inspektorów art. 38 ust. 6 RODO.

Na stronie 19 i 20 ww. Wytycznych 243 WP wskazano, że: „W praktyce często to DPO tworzy i prowadzi powyższe rejestry w oparciu o dane otrzymane od różnych departamentów organizacji odpowiedzialnych za przetwarzanie danych osobowych. Taka procedura została ustalona na mocy wielu obowiązujących przepisów państw członkowskich i przepisów o ochronie danych osobowych mających zastosowanie do instytucji i organów UE.” W odesłaniu do tego fragmentu wytycznych Grupa Robocza Art. 29 odwołała się do nieobowiązującego obecnie art. 24 (1) (d) rozporządzenia (WE) 45/2001, który określał powoływanie i zadania IOD. Zgodnie z tym przepisem prowadzenie rejestru operacji przetwarzania przeprowadzonych przez administratora należało do inspektora ochrony danych. Jednak rozporządzenie (WE) 45/2001 zostało uchylone rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE. Obecnie obowiązujące rozporządzenie 2018/1725, tak jak RODO (rozporządzenie 2016/679) wskazuje w art. 31 ust. 1, że każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. Ponadto w art. 44 ust. 6 rozporządzenia 2018/1725 odnoszącym się do statusu IOD wskazano (analogicznie jak w RODO), że inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, że takie zadania i obowiązki nie będą powodowały konfliktu interesów.

Dodatkowo należy wskazać, że praktyka prowadzenia rejestru czynności przetwarzania, o której wspominają wytyczne, nie wykształciła się na skutek stosowania przepisów RODO, lecz aktów, które obowiązywały przed wejściem do stosowania tego rozporządzenia.

W wytycznych wskazano ponadto, że: „Artykuł 39(1) określa minimalną listę zakresu obowiązków DPO. W związku z tym nic nie stoi na przeszkodzie, aby administrator lub podmiot przetwarzający powierzył DPO prowadzenie, w imieniu administratora albo podmiotu przetwarzającego, rejestru czynności przetwarzania danych."

Rzeczywiście katalog zadań inspektora ochrony danych nie jest zamknięty, niemniej w przypadku nakładania na IOD innych zadań należy zawsze uwzględnić art. 38 ust. 6 RODO, tj. że zadania nakładane przez administratora na IOD nie mogą powodować konfliktu interesów. Warto nadmienić, że takie rekomendacje co do dopuszczalności prowadzenia rejestru czynności przetwarzania przez IOD polski organ nadzorczy opublikował na swojej stronie internetowej (https://archiwum.uodo.gov.pl/pl/225/659). Wyjaśnił tam, że zgodnie z art. 30 ust. 1 i 2 RODO, do administratora należy obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, za które odpowiada, a do podmiotu przetwarzającego - prowadzenie rejestru kategorii czynności przetwarzania dokonywanych w imieniu administratora. To te podmioty są odpowiedzialne za efektywne wykonanie tego obowiązku i pozostawanie w gotowości do wykazania tego na żądanie organów ochrony danych. Natomiast inspektor ochrony danych jako fachowiec może jedynie wspomagać administratora w tworzeniu i prowadzeniu rejestrów na przykład poprzez doradzanie mu w kwestiach związanych z wykonaniem tego obowiązku.

Kolejnym zidentyfikowanym problemem była kwestia udzielenia inspektorowi ochrony danych pełnomocnictwa do występowania w imieniu administratora (reprezentowania administratora) przed organem nadzorczym i sądem w sprawach z zakresu ochrony danych osobowych. Wprawdzie polskie procedury postępowania zarówno przed sądem, jak i organem nadzorczym nie przewidują wprost wyłączenia inspektora ochrony danych z kręgu osób mogących być pełnomocnikami w sprawach z zakresu ochrony danych, ale udzielenie takiego pełnomocnictwa jest sprzeczne z zakazem nakładania na IOD zadań powodujących konflikt interesów (art. 38 ust. 6 RODO) oraz zakazem udzielania inspektorowi instrukcji co do wykonywania zadań (art. 38 ust. 3 RODO). Zadaniem pełnomocnika jest ochrona interesów mocodawcy, działanie według jego instrukcji i sugestii, co stoi w sprzeczności z zagwarantowaną w RODO niezależnością inspektora ochrony danych. Natomiast głównym celem IOD nie jest działanie wyłącznie w interesie administratora, na co wskazują zarówno zakres zadań IOD, jak i gwarancje jego niezależności. Podstawowym zadaniem IOD jest m.in. monitorowanie przestrzegania przepisów o ochronie danych osobowych przez administratora i doradzanie mu w tym zakresie. Pełnienie roli pełnomocnika

przez IOD w sprawach z zakresu ochrony danych osobowych stoi zatem w kolizji przede wszytkim z zakazem nakładania na IOD zadań powodujących konflikt interesów. IOD, działając jako pełnomocnik administratora w sprawach ochrony danych osobowych przed organem nadzorczym lub sądem, składa w imieniu mocodawcy wyjaśnienia dotyczące przetwarzania danych osobowych przez administratora. Działając zgodnie z wolą i interesem mocodawcy, w wyjaśnieniach tych mógłby być zmuszony do pomijania własnych spostrzeżeń i rekomendacji, które wypracował jako IOD. Polski organ nadzorczy w odpowiedziach na pytania inspektorów dotyczących tego zagadnienia, oprócz powyższych argumentów wskazywał, że IOD - z uwagi na swoją rolę fachowego doradcy i podmiotu monitorującego w sposób niezależny przestrzeganie przepisów o ochronie danych osobowych - powinien ze swej strony odpowiednio wcześnie identyfikować i sygnalizować administratorowi ryzyko wystąpienia takiego konfliktu. Dzięki temu możliwe jest odpowiednio wczesne zapobieganie mu. W takim przypadku inspektor ochrony danych powinien powstrzymać się od dokonywania czynności w imieniu administratora lub wypowiedzieć udzielone mu pełnomocnictwo.

Innym ważnym problemem, na który zwrócił uwagę polski organ nadzorczy, jest nieprawidłowa praktyka polegająca na zawieraniu umowy powierzenia przez administratora z IOD, który nie jest jego pracownikiem. UODO odnosił się do tego problemu, publikując na swojej stronie internetowej odpowiedzi na pytania inspektorów dotyczące tego problemu (https://archiwum.uodo.gov.pl/pl/223/2050, https://archiwum.uodo.gov.pl/pl/223/2092). Wskazywał w nich, że zawieranie umowy powierzenia przez administratora z IOD stoi w kolizji z zakazem udzielania IOD instrukcji co do wykonywania zadań i niedopuszczania do zaistnienia konfliktu interesów. Zgodnie z RODO podmiot przetwarzający jest zobowiązany do stosowania się do instrukcji przekazanych przez administratora. Natomiast w odniesieniu do inspektora ochrony danych administrator i podmiot przetwarzający mają m.in. obowiązek zapewnić, aby inspektor nie otrzymywał instrukcji dotyczących wykonywania swoich zadań (art. 38 ust. 3 RODO). Ponadto możliwość wykonywania przez osobę, z którą zawierana jest umowa o świadczenie usług, zadań innych niż określone w RODO ograniczona jest zakazem występowania w tym zakresie konfliktu interesów (art. 38 ust. 6 RODO).

Sednem ww. stanowiska jest, że występowanie inspektora ochrony danych w charakterze podmiotu przetwarzającego, który ma realizować zadania związane z przetwarzaniem danych w imieniu i na rzecz administratora oraz jest zobowiązany do stosowania się ściśle do instrukcji przekazanych mu w tym zakresie przez administratora, narusza niezależność IOD. Natomiast w relacji administrator - podmiot przetwarzający nie ma przestrzeni na niezależne działanie podmiotu przetwarzającego, w jakimkolwiek stopniu niezgodne z instrukcjami administratora. Z tego powodu IOD nie może występować w roli podmiotu przetwarzającego (być stroną umowy powierzenia) i działać na polecenie administratora, bo stoi to w sprzeczności z niezależnością inspektora gwarantowaną przez przepisy RODO.

Niezależność ta jest niezbędna, aby inspektor mógł w sposób prawidłowy realizować swoje zadania wymienione w art. 39 ust. 1 RODO.

Administratora i powołanego przez niego zewnętrznego inspektora powinna łączyć umowa o świadczenie usług, o której mowa w art. 37 ust. 6 RODO. Przedmiotem tej umowy powinny być zadania wskazane w art. 39 ust. 1 RODO, realizowane przy spełnieniu warunków określonych w przepisach tego aktu, w sposób gwarantujący inspektorowi niezależność.

Dostęp do danych osobowych niezbędnych IOD do wykonywania jego zadań wynika z przepisów prawa. Art. 38 ust. 2 RODO stanowi, że administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu m.in. dostęp do danych osobowych i operacji przetwarzania. Dotyczy to również zewnętrznego inspektora ochrony danych, wykonującego swoje zadania na podstawie umowy o świadczenie usług.

3. Czy są jakieś wiodące praktyki w organizacjach, z którymi się Państwo kontaktowali, a którymi chcieliby się Państwo podzielić?

Przeprowadzone przez UODO postępowania wyjaśniające i kontrolne wykazały, że najmniej problemów z wiarygodnym wykazaniem wypełnienia obowiązków z art. 37-39 RODO miały organizacje, które starannie przemyślały, a następnie wdrożyły w swoich regulacjach wewnętrznych konkretne, dostosowane do ich działalności zasady i sposoby postępowania w tym zakresie.

Na takie podejście administratorów i podmiotów przetwarzających oparte na zasadzie rozliczalności polski organ nadzorczy kładł nacisk już wcześniej w swoich materiałach edukacyjnych. Takie podejście przyświecało mu również przy opracowywaniu 27 pytań[1] stworzonych do weryfikacji przestrzegania przepisów dotyczących IOD. W pytaniach dotyczących np. włączania IOD w sprawy ochrony danych osobowych czy konfliktu interesów organ wskazywał, że należy przedstawić informacje na temat odpowiednich mechanizmów (rozwiązań, procedur) zapewniających przestrzeganie danego przepisu RODO.

[1] https://archiwum.uodo.gov.pl/pl/138/2336