Vademecum
Inspektora Ochrony Danych

Wydanie 1.

Rozdział I. Rola i znaczenie inspektora ochrony danych

1. Doświadczenia w wykonywaniu funkcji inspektora ochrony danych

Maciej Byczkowski

1.1. Wprowadzenie

Mija półtora roku od rozpoczęcia stosowania przepisów RODO. Dla wielu osób pełniących funkcję IOD (ang. *data protection officer* – DPO) to okres intensywnych zmian w wykonywaniu swojej pracy. Jako osoba od ponad 20 lat pełniąca najpierw funkcję administratora bezpieczeństwa informacji (ABI), a później IOD, odczułem znaczne różnice nie tylko w liczbie lub rodzaju zadań, lecz także w pozycji i postrzeganiu IOD w organizacji. Pamiętam szczególnie marzec 2018 r., kiedy w jednej z dużych organizacji, gdzie pełniłem funkcję ABI od 10 lat (całkiem spokojnie), stałem się najpopularniejszym pracownikiem, z którym wszyscy chcieli się spotkać, a do konsultacji ustawiały się długie kolejki na korytarzu przed salą spotkań. Miałem nadzieję, że to tylko „gorączka RODO", ale ten stan nadal się utrzymuje… Skąd ta zmiana? Na pewno z faktu rozpowszechnienia informacji o RODO, i pewnie też ze strachu przed konsekwencjami finansowymi (o co media dobrze zadbały). Znaczenie IOD wzrasta w organizacjach, a zależy to nie tylko od złożoności problemu przetwarzania danych u konkretnego administratora, lecz także od postawy osoby, która pełni funkcję inspektora. W niniejszym artykule przedstawię podsumowanie doświadczeń swoich oraz koleżanek i kolegów z mojego zespołu ekspertów ENSI w wykonywaniu funkcji IOD w różnych organizacjach.

1.2. Rola i znaczenie funkcji inspektora ochrony danych

RODO wprowadziło nowy wymiar dotyczący zabezpieczania przetwarzania danych osobowych przez wdrażanie odpowiednich środków technicznych i organizacyjnych,

dobieranych na podstawie szacowania ryzyka naruszenia praw lub wolności osób fizycznych (ang. *risk based approach*) oraz wykazywania zgodności przestrzegania obowiązków wynikających z RODO. Na tym tle funkcja IOD nabrała nowego znaczenia.

Grupa Robocza Art. 29 w wytycznych dotyczących inspektorów ochrony danych wskazuje, że IOD jest gwarantem rozliczalności, a jego powołanie może ułatwić przestrzeganie przepisów o ochronie danych przez administratorów oraz podmioty przetwarzające. Jej zdaniem wyznaczenie IOD ma kluczowe znaczenie w procesie przetwarzania danych w organizacji, stąd w RODO szczegółowo określono warunki jego wyznaczenia, status oraz zadania. Podkreśla również, że IOD odgrywa rolę pośredniczącą pomiędzy administratorem danych a osobami, których dane dotyczą, jak również pomiędzy administratorem danych a organem nadzorczym[1].

Zgodnie z motywem 97 RODO inspektor to osoba, która ma wspomagać administratora danych lub podmiot przetwarzający w monitorowaniu wewnętrznego przestrzegania RODO, a tym samym w wykazywaniu zgodności przestrzegania obowiązków RODO. Wymagana bezpośrednia podległość najwyższemu kierownictwu administratora lub podmiotu przetwarzającego oraz niezależność w wykonywaniu swoich obowiązków i zadań wskazuje, że osoba ta ma być partnerem dla zarządzających przy zapewnieniu przestrzegania obowiązków ochrony danych osobowych. Jednak to, jak jest w rzeczywistości, wie każdy IOD. Wiele zależy od poziomu świadomości zarządzających w odniesieniu do wagi problemu ochrony danych w organizacji. Problemem są też stare przyzwyczajenia i przeświadczenie, że dawny ABI, a obecny IOD jest raczej wykonawcą, mającym rozwiązywać każdy problem dotyczący ochrony danych i odpowiadającym za ochronę danych osobowych w organizacji. Niemniej sam fakt wyznaczenia takiej osoby, wymuszony w wielu przypadkach przepisami RODO, daje szansę na zapewnienie przestrzegania przepisów o ochronie danych osobowych przy ich przetwarzaniu w organizacji administratora lub podmiotu przetwarzającego.

Należy podkreślić, że znaczenie funkcji IOD wzrosło w stosunku do wcześniejszej funkcji ABI. Przede wszystkim dotyczy to pełnienia funkcji punktu kontaktowego dla osób, których dane dotyczą, uczestnictwa w zgłaszaniu sytuacji naruszenia ochrony danych do Prezesa UODO, jak również uczestnictwa w procesie oceny skutków dla ochrony danych – co nie było określone we wcześniejszych przepisach o ochronie danych obowiązujących w Polsce. Natomiast co do statusu IOD – jeśli chodzi o jego podległość najwyższemu kierownictwu administratora i niezależność w wykonywaniu zadań oraz główny zakres tych zadań – polskie przepisy o ochronie danych były zbieżne z wymaganiami RODO już od 1.1.2015 r. Dzięki temu powołani ABI mogli przygotować się zawczasu do pełnienia nowej funkcji IOD[2].

Najistotniejsze w pełnieniu funkcji IOD jest nie tylko posiadanie odpowiednich kwalifikacji zawodowych zgodnie z art. 37 ust. 5 RODO, lecz również odpowiednia postawa osoby pełniącej tę funkcję. Chodzi o postawę etyczną tej osoby, która daje gwarancję, że

[1] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych ('DPO') (WP 243, rew.01), przyjęte 13.12.2016 r., ostatnio zmienione i przyjęte 5.4.2017 r., https://uodo.gov.pl/data/filemanager_pl/15.pdf (dostęp: 8.11.2019 r.), s. 1–2.

[2] Więcej *M. Byczkowski*, Przygotowanie ABI do nowej funkcji inspektora ochrony danych, Informacja w Administracji Publicznej 2017, Nr 1.

prawo do prywatności osób, których dane są przetwarzane, będzie przestrzegane. Osoba taka powinna chronić prywatność osób nie tylko w pracy, ale również na co dzień. Nie możemy zapominać, że prawo do prywatności to jedno z podstawowych praw każdego człowieka – zawarte również w art. 12 Powszechnej Deklaracji Praw Człowieka[3]. Drogowskazem w tym zakresie jest Kodeks etyki inspektora ochrony danych, opracowany i przyjęty przez SABI – Stowarzyszenie Inspektorów Ochrony Danych[4]. Zgodnie z tym kodeksem IOD powinien kierować się zasadami etyki, którymi w szczególności są:

1) zasada prawości,
2) zasada obiektywizmu,
3) zasada niezależności,
4) zasada profesjonalizmu,
5) zasada poufności,
6) zasada unikania konfliktu interesów.

Przestrzeganie przez IOD zasad etyki zawodowej i wypełnianie standardów postępowania jest gwarancją wysokiego poziomu ochrony praw i wolności osób, których dane są przetwarzane.

1.3. Praktyka związana z wyznaczaniem inspektora ochrony danych

1.3.1. Obowiązek wyznaczenia inspektora ochrony danych

Przepisy RODO wprowadziły obowiązek wyznaczenia IOD w konkretnych sytuacjach. Jest o nich mowa w motywie 97 oraz art. 37 ust. 1 RODO. Zgodnie z przepisami inspektora muszą wyznaczać:

1) organy i podmioty publiczne (z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości);
2) podmioty, których główna działalność wiąże się z przetwarzaniem danych osobowych, a ich przetwarzanie wymaga regularnego i systematycznego monitorowania osób, których dotyczą na dużą skalę;
3) podmioty, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych określonych w art. 9 RODO lub danych dotyczących wyroków skazujących i czynów zabronionych określonych w art. 10 RODO.

Pozostali administratorzy lub podmioty przetwarzające, którzy nie kwalifikują się do wskazanych wyżej kategorii, mogą wyznaczyć IOD.

[3] Powszechna Deklaracja Praw Człowieka – przyjęta 10.12.1948 r. rezolucją 217/III A Zgromadzenia Ogólnego ONZ w Paryżu – Ośrodek Informacji ONZ w Warszawie, http://www.unic.un.org.pl/dokumenty/deklaracja.php (dostęp: 8.11.2019 r.).

[4] Kodeks Etyki Inspektora Ochrony Danych – przyjęty 30.1.2018 r. uchwałą Nadzwyczajnego Walnego Zgromadzenia SABI – Stowarzyszenia Inspektorów Ochrony Danych, https://sabi.org.pl/KodeksEtyki.php (dostęp: 8.11.2019 r.).

O ile w przypadku podmiotów czy organów publicznych nie było dyskusji na temat obowiązku wyznaczenia IOD, o tyle już w podmiotach prywatnych zauważyłem tendencję do uciekania od obowiązku wyznaczania IOD. Spotykałem się z pytaniami od klientów, którzy przetwarzali duże ilości danych i wykonywali operacje przetwarzania kwalifikujące się do przeprowadzania oceny skutków dla ich ochrony zgodnie z art. 35 RODO, typu: „Co zrobić, aby nie musieć wyznaczać IOD?". W świetle wymagań RODO oraz przewidzianych konsekwencji prawnych i finansowych takie działania są ryzykowne i nieodpowiedzialne. Można zadać pytanie: „Kogo stać dziś na funkcjonowanie bez IOD?". Administratorzy i podmioty przetwarzające nie uciekną przecież od obowiązków związanych z zapewnieniem przestrzegania RODO i rozliczaniem się z wykonywania tych obowiązków. Wyznaczony IOD może ich w tym skutecznie wspierać i minimalizować ryzyko wystąpienia prawnych i finansowych konsekwencji, związanych z niewłaściwym przetwarzaniem danych lub brakiem ich ochrony. Zatem **wyznaczenie IOD staje się biznesową koniecznością** i może również wpisywać się w politykę społecznej odpowiedzialności biznesu (ang. *Corporate Social Responsibility* – CSR) przyjętej przez danego administratora danych.

Aby móc właściwie wyznaczyć IOD, administrator danych lub podmiot przetwarzający powinien na początku podjąć następujące czynności:

1) określić, czy IOD będzie wykonywał zadania na wyodrębnionym stanowisku, czy na podstawie powierzenia mu funkcji, oraz wskazać odpowiednie dla niego miejsce w strukturze organizacji;
2) określić zasady rekrutacji IOD, w tym zasady potwierdzania wymaganych kwalifikacji i potrzebnych kompetencji do wykonywania zadań;
3) określić potrzebne uprawnienia dla IOD, niezbędne do wykonywania jego obowiązków;
4) określić potrzebę wyznaczenia zastępców IOD oraz powołania zespołu IOD.

1.3.2. Inspektor ochrony danych jako funkcja lub stanowisko

RODO nie wymaga, aby administrator lub podmiot przetwarzający wyznaczył IOD na wyodrębnionym stanowisku. Zależy to od wewnętrznej decyzji tych podmiotów, jak również od szczególnych przepisów określających wykazy stanowisk w podmiotach publicznych. Zatem IOD może, lub w pewnych przypadkach musi, być wyznaczony na niezależnym stanowisku. Nic nie stoi jednak na przeszkodzie, aby funkcję IOD powierzyć osobie zatrudnionej na innym stanowisku. W tym drugim przypadku należy rozważyć, czy powierzenie funkcji IOD nie rodzi konfliktu interesów. Można również skorzystać z opcji outsourcingu funkcji IOD.

W praktyce najczęściej spotykanym rozwiązaniem jest powierzanie funkcji IOD osobom zatrudnionym na innych stanowiskach. Nie ma tu reguły – wyznaczani IOD są zatrudniani na różnych stanowiskach. Dobrze jest, aby osoba wyznaczona do pełnienia funkcji IOD wykonywała zadania zbieżne z ochroną danych osobowych, np. związane z bezpieczeństwem innych rodzajów informacji czy z audytem wewnętrznym. Kluczową kwestią jest zapewnienie niezależności w wykonywaniu zadań IOD, dlatego tak istotne jest to, aby inne zadania, które wykonuje inspektor, nie kolidowały z wykonywaniem zadań IOD określonych w RODO. W takiej sytuacji istotna jest też podległość służbowa. Jeżeli przełożony osoby wyznaczonej do pełnienia funkcji IOD nie będzie zapewniać możliwości wykonywania przez nią zadań, to takie wyznaczenie będzie w tym wypadku fikcją.

Warto zwrócić uwagę na szczególne przepisy, które odnoszą się do funkcji IOD jako specjalności zawodowej. Inspektor ochrony danych znalazł się w klasyfikacji zawodów i specjalności na potrzeby rynku pracy, opublikowanej w KlasZawRynekR (jest wymieniony w grupie specjalistów ds. zarządzania i organizacji)[5]. Można zatem traktować funkcję IOD jako uznaną specjalność rynkową.

Może się zdarzyć, że funkcja IOD znajdzie się w wykazie stanowisk urzędowych w sferze publicznej. Wówczas IOD będzie nie tylko wyznaczony, lecz także zatrudniony na wyodrębnionym stanowisku. Przykładem są przepisy dotyczące stanowisk i szczegółowych zasad wynagradzania urzędników i innych pracowników sądów i prokuratury, wprowadzające stanowisko inspektora ochrony danych w sądach powszechnych i wojskowych[6]. Co ciekawe w tym wypadku wymaga się, żeby IOD miał ukończone studia drugiego stopnia. Innym przykładem jest wykaz stanowisk urzędniczych w Biurze Krajowej Rady Radiofonii i Telewizji. Od osoby zatrudnionej na stanowisku IOD wymaga się wykształcenia wyższego magisterskiego oraz 7 lat pracy (w tym na stanowisku kierowniczym)[7].

1.3.3. Zasady rekrutacji inspektora ochrony danych

Aby móc wybrać właściwego IOD, należy ustalić odpowiednie zasady jego rekrutacji. Przepisy art. 37 ust. 5 RODO wymagają, aby kandydaci do pełnienia funkcji IOD posiadali odpowiednie kwalifikacje zawodowe, w tym wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych, oraz umiejętności wypełniania zadań IOD, o których mowa w art. 39 RODO. Do pełnienia funkcji IOD przydatne są w szczególności następujące kompetencje:

1) umiejętności z zakresu prowadzenia audytu wewnętrznego,
2) wiedza z zakresu szacowania ryzyka,
3) wiedza dotycząca funkcjonowania systemu informatycznego,
4) umiejętności związane z opracowywaniem dokumentacji dotyczącej ochrony danych,
5) umiejętności związane z prowadzeniem szkoleń.

Do potwierdzenia wiedzy z ochrony danych mogą być przydatne różnego rodzaju dyplomy, zaświadczenia czy certyfikaty ukończenia specjalistycznych szkoleń, warsztatów, kursów czy studiów w zakresie przetwarzania danych zgodnie z RODO czy wykonywania zadań IOD. Natomiast do potwierdzenia umiejętności wypełniania zadań IOD lub dodatkowych kompetencji, szczególnie w przypadku osób, które nie pełniły wcześniej takiej funkcji, pomocne będą programy odbytych kursów, warsztatów lub studiów, z których wynika, że kandydat przechodził szkolenie praktyczne z wykonywania poszczególnych zadań IOD w formie warsztatowej. Jeśli chodzi o kandydatów, którzy pełnili wcześniej

[5] Załącznik Nr 1, pozycja 242111.

[6] Załącznik Nr 1 do rozporządzenia Ministra Sprawiedliwości z 16.5.2018 r. zmieniającego rozporządzenie w sprawie stanowisk i szczegółowych zasad wynagradzania urzędników i innych pracowników sądów i prokuratury oraz odbywania stażu urzędniczego (Dz.U. z 2018 r. poz. 1001), kolumna 1, wiersz 3 – pozostałe stanowiska wspomagające.

[7] Załącznik Nr 1 do rozporządzenia Prezydenta Rzeczypospolitej Polskiej z 28.6.2019 r. w sprawie określenia stanowisk urzędniczych, zasad wynagradzania oraz wymaganych kwalifikacji zawodowych pracowników Biura Krajowej Rady Radiofonii i Telewizji (Dz.U. z 2019 r. poz. 1234), kolumna 1, wiersz 4, poz. 3.

funkcję IOD, kluczowe jest dobre CV, z wykazem zadań realizowanych u danego administratora oraz listy z referencjami. Przy rekrutacji IOD przez podmioty z konkretnej branży istotna będzie również znajomość jej specyfiki, w tym przepisów prawa odnoszących się do niej. W celu potwierdzenia kompetencji posiadanych przez kandydatów na IOD można przeprowadzać testy sprawdzające.

1.3.4. Nadawanie inspektorowi ochrony danych odpowiednich uprawnień

W celu zapewnienia właściwej realizacji zadań przez IOD należy nadać mu niezbędne uprawnienia. W zakresie potrzebnych uprawnień można wskazać w szczególności:

1) możliwość monitorowania przestrzegania ochrony danych oraz audytów zgodności z wymaganiami RODO w komórkach organizacyjnych administratora lub podmiotu przetwarzającego;
2) prawo żądania wglądu w dokumentację dotyczącą przetwarzania danych, w tym umowy z klientami (osobami fizycznymi), kontrahentami, podmiotami przetwarzającymi, procedury, instrukcje, wzory formularzy do zbierania danych, dokumentację z danymi osobowymi;
3) prawo wglądu do systemu informatycznego, służącego do przetwarzania danych;
4) prawo wykonywania audytów w podmiotach przetwarzających w odniesieniu do zawartych umów powierzenia przetwarzania danych lub do weryfikacji takich podmiotów pod kątem zapewnianych gwarancji wypełniania wymogów RODO przed podpisaniem takiej umowy;
5) pełnomocnictwo do zgłaszania naruszeń ochrony danych do Prezesa UODO w imieniu administratora danych.

Oprócz szczególnych pełnomocnictw uprawnienia mogą być określone w dokumencie wyznaczającym IOD lub wynikać z regulaminu organizacyjnego czy dokumentacji polityki ochrony danych przyjętych przez administratora lub podmiot przetwarzający.

1.3.5. Wyznaczanie zastępcy oraz powoływanie zespołu inspektora ochrony danych

Przepisy RODO nie definiują ani nie określają funkcji zastępcy IOD. Natomiast na podstawie OchrDanychU, uzupełniającej RODO, od 4.5.2019 r. istnieje możliwość wyznaczania osoby zastępującej IOD. Pojawienie się takiego przepisu jest dobrą kontynuacją tradycji powoływania zastępcy ABI, która wynikała z poprzednich przepisów ochronie danych osobowych, obowiązujących w Polsce do 24.5.2018 r. Wielu administratorów danych powoływało zastępców ABI, którzy wykonywali jego zadania podczas jego nieobecności. Dzięki temu zadania dotyczące zapewniania przestrzegania przepisów o ochronie danych mogły być w takim podmiocie kontynuowane. Przepisy nie ograniczały liczby osób, które mogły być powołane na zastępców. Kiedy pełniłem funkcję ABI w różnych podmiotach, często sam miałem powołanych kilku zastępców, którzy wchodzili w skład mojego zespołu.

Przepis art. 11a OchrDanychU daje możliwość wyznaczenia osoby zastępującej IOD, ale zastępstwo to ogranicza się jedynie do czasu nieobecności IOD. Powoduje to

zamieszanie organizacyjne, ponieważ wyznaczenie i odwołanie zastępcy IOD należy zgłaszać Prezesowi UODO – art. 10 ust. 1 OchrDanychU stosuje się bowiem również do zgłaszania zastępców. Podmiot, który wyznaczył taką osobę, ma zawiadomić Prezesa UODO o jej wyznaczeniu w ciągu 14 dni. Jeżeli więc IOD jest nieobecny np. przez tydzień, to zanim pismo z zawiadomieniem trafi do urzędu, IOD może już wrócić, a w efekcie trzeba będzie odwołać jego zastępcę. Innym problemem jest konieczność wprowadzania adekwatnych zmian w informacjach o wyznaczonym IOD na stronie internetowej administratora lub podmiotu przetwarzającego. Lepszym rozwiązaniem byłoby wyznaczenie osoby zastępującej IOD na stałe lub kilku takich osób, które pełniłyby swoją funkcję przy każdej nieobecności IOD (zwłaszcza że zgodnie z art. 37 ust. 5 RODO na zastępcę IOD można wyznaczyć jedynie osoby posiadające takie same kwalifikacje jak IOD, a może ich zabraknąć w organizacji wtedy, gdy będą potrzebne). Problem ciągłości wykonywania funkcji IOD jest istotny z punktu widzenia realizacji obowiązków administratora lub podmiotu przetwarzającego zgodnie z RODO. Mam więc nadzieję, że przepis art. 11a OchrDanychU zostanie doprecyzowany lub organ nadzorczy ustali właściwą praktyk**ę**.

Dobrym rozwiązaniem jest powołanie zespołu IOD, jeżeli są takie możliwości organizacyjne i finansowe. W skład zespołu mogą wchodzić osoby o niezbędnych kompetencjach z zakresu prawa, organizacji i zarządzania oraz bezpieczeństwa IT. Gdy pełnię funkcję IOD w ramach outsourcingu, zapewniam swoim klientom taki interdyscyplinarny zespół, który pozwala mi podejmować niezbędne działania doradcze w różnych obszarach w celu zapewnienia realizacji obowiązków RODO. W zespole są również wskazani zastępcy IOD. Na możliwość powołania zespołu IOD zwraca uwagę również Grupa Robocza Art. 29 w swoich wytycznych dotyczących IOD, w szczególności przy wyznaczeniu jednego IOD dla wielu podmiotów[8].

1.3.6. Inspektor ochrony danych w grupach kapitałowych

Wyznaczenie jednego wspólnego IOD w kilku podmiotach wchodzących w skład grupy kapitałowej, w tym międzynarodowej, jest dopuszczalne zgodnie z art. 37 ust. 2 RODO. Taka decyzja wymaga bezwzględnie powołania również zespołu IOD ze względu na zapewnienie możliwości wykonywania zadań IOD w grupie (bez takiego wsparcia wspólny IOD będzie fikcją). Co prawda przepis art. 37 ust. 2 RODO wskazuje, że powołanie wspólnego IOD jest uwarunkowane łatwością nawiązywania z nim kontaktu z każdego podmiotu, lecz i tak w każdym z tych podmiotów powinien być wyznaczony koordynator ds. ochrony danych, który wejdzie w skład zespołu IOD lub będzie wyznaczony na zastępcę IOD w danym podmiocie.

RODO nie daje wskazówek co do tego, w jaki sposób IOD ma być zatrudniony przez spółki z grupy. Może być on pracownikiem każdej ze spółek zatrudnionym na część etatu bądź świadczyć dla nich pracę w ramach umów cywilnoprawnych. W tym zakresie podmioty mają swobodę. Spółki z grupy mogą podpisać wspólne porozumienie dotyczące

[8] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych…, s. 11–12 i 15.

wyznaczenia jednego IOD. Mogą być również wprowadzone odpowiednie postanowienia do polityki ochrony danych w grupie kapitałowej. W porozumieniu należy ustalić, jak będą rozliczane koszty dotyczące IOD w grupie. Jeżeli będzie on zatrudniony przez jedną ze spółek, np. spółkę matkę, to zapewni ona oprócz wynagrodzenia również niezbędne środki do wykonywania funkcji IOD. Należy zatem ustalić, czy w związku z tym pozostałe spółki-córki zostaną obciążone kosztami administracyjnymi w tym zakresie. Należy pamiętać, że każda ze spółek ma obowiązek odrębnie powiadomić Prezesa UODO o wyznaczeniu IOD, zgodnie z wymaganiami art. 10 OchrDanychU, oraz opublikować informację o wyznaczonym IOD zgodnie z art. 11 OchrDanychU.

Innym rozwiązaniem, które spotykam w grupach kapitałowych, jest wyznaczanie odrębnych IOD dla każdej ze spółek i powołanie wspólnego zespołu inspektorów dla grupy kapitałowej, którego przewodniczącym zwykle jest IOD w spółce matce. Taki zespół ustala wspólne standardy i wytyczne dotyczące zapewnienia przestrzegania przepisów RODO w grupie. W art. 37 ust. 3 RODO dopuszczono także powołanie jednego wspólnego IOD dla kilku organów lub podmiotów publicznych, po uwzględnieniu ich struktury organizacyjnej i wielkości. Przy realizacji takiego rozwiązania można korzystać z praktyki grup kapitałowych, opisanej powyżej.

1.3.7. Publikowanie danych kontaktowych inspektora ochrony danych i zawiadamianie o nich Prezesa Urzędu Ochrony Danych Osobowych

Zgodnie z art. 37 ust. 7 RODO w razie wyznaczenia IOD administrator lub podmiot przetwarzający ma obowiązek opublikowania danych kontaktowych IOD oraz przekazaniu ich w zawiadomieniu do Prezesa UODO. Zakres wykonania tych obowiązków doprecyzowuje OchrDanychU. Przepisy art. 10 OchrDanychU określają sposób postępowania przy realizacji obowiązku powiadomienia Prezesa UODO. Szczegółowe informacje wraz ze wzorami zawiadomień i sposobem ich wykonania znajdują się na stronie internetowej UODO[9].

Zgodnie z art. 11 OchrDanychU administrator lub podmiot przetwarzający, niezwłocznie po wyznaczeniu IOD, udostępnia jego dane na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności (np. na tablicy ogłoszeń przy wejściu do siedziby, w treści klauzuli informacyjnej dotyczącej monitoringu wizyjnego lub w treści klauzuli dotyczącej przetwarzania danych osobowych gości wchodzących na jego teren). Zakres tych danych obejmuje: imię, nazwisko oraz adres e-mail lub numer telefonu. Ponieważ publikacja danych kontaktowych IOD ma na celu umożliwienie nawiązania z nim kontaktu, powinny być one widoczne, a nie ukryte. Dlatego na głównej stronie powinna być widoczna zakładka np. „Dane osobowe", „Ochrona danych", „Inspektor ochrony danych", „RODO" itp. Dane IOD mogą być też podane w polityce prywatności zamieszczonej na stronie internetowej.

[9] Zob. Urząd Ochrony Danych Osobowych, Zawiadomienia Prezesa UODO związane z IOD, https://uodo.gov.pl/p/zawiadomienia-prezesa-uodo-zwiazane-z-iod (dostęp: 8.11.2019 r.).

Informację o IOD wraz z wymaganymi danymi kontaktowymi należy przekazać również pracownikom podmiotu, w którym został on wyznaczony. W tym celu można zamieścić stosowną informację w wewnętrznym intranecie, w książce telefonicznej, w kontaktach w systemie poczty elektronicznej czy w schematach dotyczących struktury organizacyjnej danego administratora lub podmiotu przetwarzającego. **Brak opublikowania wymaganych danych IOD czy publikacja niepełnych danych (np. bez imienia i nazwiska) jest naruszeniem wymogów RODO oraz OchrDanychU** – co niestety często można zauważyć.

1.4. Praktyka związana z zapewnieniem wymaganego statusu inspektora ochrony danych

Obowiązek wyznaczenia IOD lub decyzja o jego dobrowolnym wyznaczeniu przez administratora lub podmiot przetwarzający są ściśle związane z koniecznością zapewnienia odpowiedniego statusu IOD. Niedopełnienie tego obowiązku świadczy o braku zrozumienia przepisów RODO przez te podmioty, a ponadto jest zagrożone administracyjnymi karami pieniężnymi zgodnie z art. 83 ust. 4 lit. a RODO. Podkreślam to nie bez powodu – samo wyznaczenie IOD bez zapewnienia mu odpowiedniego statusu jest w zasadzie formą oszustwa. Osoba wyznaczona na IOD nie może bowiem wykonywać swoich obowiązków określonych w RODO, a jeżeli godzi się na to, można uznać, że jest współwinna. Niestety z realizacją wymogów dotyczących zapewnienia statusu IOD administratorzy danych i podmioty przetwarzające mają najwięcej problemów. W tym wypadku dużo zależy też od postawy samego IOD, jego aktywności i determinacji do zapewnienia sobie właściwego i zgodnego z RODO statusu.

1.4.1. Włączanie inspektora ochrony danych we wszystkie sprawy dotyczące przetwarzania danych

Zgodnie z wymogiem art. 38 ust. 1 RODO administrator oraz podmiot przetwarzający mają zapewnić, aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Jest to istotne szczególnie przy realizacji obowiązków dotyczących uwzględniania ochrony danych w fazie projektowania czy przy ocenie skutków dla ochrony danych w przypadku planowania nowych operacji przetwarzania danych. Mimo stosowania RODO od wielu miesięcy omawiany obowiązek nie jest spełniany w znacznej większości podmiotów. Z jednej strony, wynika to z braku świadomości, że takie sprawy powinny być konsultowane z IOD, a z drugiej – z braku kultury ochrony danych osobowych w organizacjach. W rzeczywistości IOD dowiaduje się więc o wielu sprawach, procesach czy projektach często w ostatniej chwili albo podczas okresowego audytu zgodności procesów przetwarzania danych z RODO.

Aby zapewnić realizację tego obowiązku, potrzebna jest ciągła akcja informacyjna i szkoleniowa. Inspektor powinien realizować ją z poparciem kierownictwa administratora lub podmiotu przetwarzającego. Istotne jest także wdrożenie odpowiednich procedur, w ramach polityki ochrony danych, które będą obowiązywać wszystkie osoby dopuszczone

do przetwarzania danych. W polityce lub procedurach należy wprowadzić obowiązek zapraszania IOD na spotkania organizowane przez najwyższe kierownictwo oraz poszczególne komórki organizacyjne administratora lub podmiotu przetwarzającego, podczas których są omawiane kwestie lub podejmowane decyzje związane z przetwarzaniem danych osobowych w ramach bieżących lub projektowanych procesów realizowanych w organizacji. W razie gdy udział IOD w spotkaniu jest niemożliwy, należy zobowiązać organizatora do przesłania IOD notatki zawierającej poruszone problemy dotyczące przetwarzania danych osobowych.

Inspektor powinien uczulać na omawiany problem kierowników komórek organizacyjnych, odpowiedzialnych za procesy przetwarzania danych, lub ich pracowników podczas realizacji zadań związanych z monitorowaniem, w tym audytów zgodności z RODO w odniesieniu do procesów wpisanych do rejestru czynności przetwarzania danych osobowych, jak również podczas przeprowadzania szacowania ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Istotne jest to, aby przy wykonywaniu tych zadań IOD wzbudzał zarówno zaufanie, jak i respekt.

1.4.2. Zapewnienie inspektorowi ochrony danych zasobów do realizacji zadań

Bez niezbędnych zasobów potrzebnych do wykonywania zadań, odpowiednich uprawnień w zakresie dostępu do danych osobowych oraz informacji na temat operacji ich przetwarzania IOD będzie jak bezzębny tygrys. Administrator oraz podmiot przetwarzający w ramach obowiązków wynikających z art. 38 ust. 2 RODO powinni zapewnić IOD w szczególności:

1) odpowiednie miejsce pracy, sprzęt komputerowy i oprogramowanie niezbędne do realizacji zadań,
2) wsparcie w postaci oddelegowania osób do pomocy, w tym (w zależności od potrzeb) – powołanie zespołu IOD,
3) wsparcie w zakresie komunikowania w organizacji problemów związanych z ochroną danych oraz zatwierdzania i wdrażania odpowiednich polityk, procedur lub wytycznych w zakresie ochrony danych,
4) uprawnienia do wykonywania zadań związanych z monitorowaniem przetwarzania danych, w tym dostęp do nośników, pomieszczeń oraz systemów IT, w których są przetwarzane dane,
5) budżet na szkolenia doskonalące i warsztaty dotyczące wykonywania zadań IOD,
6) budżet na specjalistyczne konsultacje prawne, techniczne/informatyczne lub organizacyjne,
7) możliwość uczestnictwa w środowiskowych konferencjach lub seminariach,
8) pełnomocnictwa do reprezentowania podmiotu przed Prezesem UODO, m.in. w sytuacjach naruszenia ochrony danych,
9) umożliwienie zgłaszania potrzeb w zakresie niezbędnych zasobów finansowych, organizacyjnych, sprzętowych i kadrowych.

Zrealizowanie powyższych postulatów, jak również innych w zależności od potrzeb, zależy od inicjatywy IOD oraz umiejętności negocjowania w tym zakresie z najwyższym kierownictwem administratora lub podmiotu przetwarzającego.

1.4.3. Zapewnienie inspektorowi ochrony danych możliwości wykonywania zadań

Zgodnie z art. 38 ust. 6 RODO inspektor nie może wykonywać dodatkowych obowiązków, które powodowałyby konflikt interesów, w szczególności gdy wpływa to na prawidłowe wykonywanie zadań IOD. Dotyczy to zarówno IOD wyznaczonego na niezależnym stanowisku, jak i osoby zatrudnionej na innym stanowisku, której powierzono pełnienie funkcji IOD. Szczególnie w pierwszym przypadku, gdy osoba pełni tylko funkcję IOD, mogą zdarzać się próby „dociążania" jej dodatkowymi zadaniami. Jest to dopuszczalne, pod warunkiem że charakter tych zadań jest zbieżny z wykonywaniem obowiązków IOD w zakresie monitoringu przepisów RODO, np. prowadzenie dokumentacji dotyczącej przetwarzania danych czy rejestrów czynności przetwarzania danych osobowych.

Grupa Robocza Art. 29 wskazuje, że konflikt interesów pojawia się w przypadku wykonywania przez IOD obowiązków na stanowiskach, które polegają na decydowaniu o celach i sposobach przetwarzania danych osobowych – w tym na stanowiskach kierowniczych (np. dyrektora generalnego, dyrektora operacyjnego, kierownika działu HR lub IT itp.)[10]. Należy o tym pamiętać, gdy administrator lub podmiot przetwarzający zamierzają wyznaczyć do pełnienia funkcji IOD osobę, która jest zatrudniona na tego rodzaju stanowisku. Istnienie konfliktu interesów powinno być sprawdzane przez kierownika działu HR przed wyznaczeniem IOD lub wprowadzeniem zmian w zakresie jego obowiązków. W wielu wypadkach konflikt interesów pojawia się dlatego, że nie wykonuje się tzw. testów równowagi w sytuacji łączenia różnych stanowisk z funkcją IOD.

Ważne

Gdy IOD ma uzasadnione podejrzenie możliwości zaistnienia konfliktu interesów przy wykonywaniu przez niego powierzonych zadań, ma obowiązek zgłosić to zarządowi lub kierownikowi jednostki organizacyjnej administratora danych. Powinien to robić we własnym interesie, aby móc rozliczyć się z prawidłowego wykonywania swoich obowiązków określonych w RODO.

1.4.4. Zapewnienie inspektorowi ochrony danych niezależności i odpowiedniej podległości

Zapewnienie niezależności wykonywania funkcji IOD, o której mowa w motywie 97 RODO, jest gwarancją prawidłowego wykonywania jego zadań, bez względu na to, czy IOD jest pracownikiem administratora danych, czy wykonuje swoją funkcję w ramach outsourcingu. Przy outsourcingu niezależność IOD łatwiej jest zapewnić odpowiednimi

[10] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych…, s. 17.

zapisami w umowie i wykazać ją w praktyce. Również w przypadku wyznaczenia do pełnienia funkcji IOD osoby na niezależnym stanowisku niezależność może być zapewniona bez problemu. Natomiast przy łączeniu stanowisk z funkcją IOD mogą pojawiać się problemy z niezależnością ze względu na możliwą zdublowaną podległości takiej osoby w strukturze organizacyjnej administratora lub podmiotu przetwarzającego. Przy zapewnianiu niezależności IOD należy pamiętać o właściwym stosowaniu wymogów określonych w art. 38 ust. 3 RODO, w tym o:

1) niewydawaniu IOD instrukcji dotyczących realizacji jego zadań, określonych w art. 39 RODO,
2) nieodwoływaniu i niekaraniu IOD za wypełnianie zadań (oczywiście prawidłowe),
3) podległości IOD najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

Szczególną sytuacją dotyczącą konieczności zapewnienia niezależności IOD jest jego relacja z komórką audytu wewnętrznego administratora lub podmiotu przetwarzającego. Audytorzy wewnętrzni nie mogą ingerować w decyzje IOD ani podważać jego rekomendacji w sprawach związanych z przetwarzaniem danych osobowych i wniosków z przeprowadzanego monitorowania zgodności przetwarzania danych z RODO. Audytor wewnętrzny ma prawo natomiast zweryfikować, czy IOD wykonuje swoje zadania określone np. w polityce ochrony danych czy regulaminie funkcji IOD.

1.4.5. Zapewnienie osobom, których dane dotyczą kontaktu z inspektorem ochrony danych

Na potrzeby realizacji zadania pełnienia przez IOD punktu kontaktowego dla podmiotów danych, o którym mowa w art. 38 ust. 4 RODO, administrator powinien zapewnić możliwość takiego kontaktu. W tym wypadku ma on obowiązek podjęcia działań w dwóch obszarach. Po pierwsze, musi publikować na swojej stronie internetowej aktualne dane kontaktowe IOD – w tym jego imię, nazwisko oraz adres e-mail lub numer telefonu. Po drugie, powinien w uporządkowany sposób podawać dane kontaktowe IOD, w ramach realizacji obowiązków informacyjnych przy zbieraniu danych zgodnie z art. 13 i 14 RODO. W klauzulach informacyjnych wystarczy podawać aktualny adres e-mail lub numer telefonu służbowego IOD, bez podawania imienia i nazwiska. Zaleca się podawanie ogólnej skrzynki, typu: iod@firma.pl, którą w zależności od potrzeb będzie przeglądać IOD lub osoba go zastępująca (albo inne osoby z zespołu IOD).

Spotkałem się z sytuacjami, gdy w klauzulach informacyjnych, wydrukowanych na różnego rodzaju formularzach do zbierania danych lub wywieszanych w punktach sprzedaży, podawano: imię, nazwisko, adres korespondencyjny czy nazwę firmy outsourcingowej zatrudniającej IOD oraz numer telefonu i adres e-mail. Nie ma zakazu podawania tak szerokiego zakresu danych kontaktowych IOD, ale trzeba pamiętać, że w razie zmiany IOD będzie konieczność zaktualizowania rozesłanych informacji, a to może być dużym problemem logistycznym (zwłaszcza że w wielu przypadkach klauzule były udostępniane w formie papierowej lub rozsyłane pocztą elektroniczną).

Dane kontaktowe do IOD powinny być znane również pracownikom infolinii lub call center, na wypadek gdyby osoba, której dane dotyczą, potrzebowała się z nim skontaktować.

1.5. Realizacja zadań przez inspektora ochrony danych

Zakres zadań, które ma obowiązek wykonywać IOD, wynika z różnych przepisów RODO, w tym z art. 39 ust. 1 oraz art. 38 ust. 4 i 6 RODO. Powinien być on dokładnie określony, np. w załączniku dołączonym do uchwały wyznaczającej IOD, w wykazie zadań opisanych w dokumencie polityki ochrony danych lub w regulaminie funkcji IOD. Jest to w interesie samego IOD, ponieważ powinien on móc rozliczać się z wykonywanych zadań. Muszą być one tak szczegółowo opisane, aby nie powodować niepotrzebnych zarzutów niewłaściwego wykonywania obowiązków przez IOD.

Zadania IOD określone w art. 39 ust. 1 RODO można podzielić na dwie grupy pod względem częstotliwości ich wykonywania:

1) zadania główne – realizowane na co dzień lub okresowo,
2) pozostałe zadania – realizowane incydentalnie w zależności od zaistnienia potrzeby.

1.5.1. Zadania główne inspektora ochrony danych

Zadania główne powinny być wykonywane przez IOD w sposób usystematyzowany. Do zadań głównych należą:

1) informowanie kierownictwa administratora lub podmiotu przetwarzającego oraz osób upoważnionych do przetwarzania danych o obowiązkach wynikających z RODO oraz przepisach uzupełniających RODO,
2) doradzanie kierownictwu oraz osobom upoważnionym w zakresie realizacji obowiązków RODO związanych z przetwarzaniem danych w organizacji,
3) monitorowanie przestrzegania przepisów RODO oraz zasad określonych w politykach ochrony danych wdrożonych w danej organizacji.

Ad 1. W zakresie realizacji zadania związanego z informowaniem kierownictwa oraz osób upoważnionych w pierwszej kolejności IOD powinien skupić się na przygotowaniu odpowiednich materiałów informacyjnych oraz ustaleniu reguł przeprowadzania szkoleń wstępnych, stanowiskowych lub okresowych z zasad ochrony danych w organizacji. W praktyce materiały informacyjne dotyczące przepisów o ochronie danych oraz wprowadzonych zasad ochrony w ramach polityki ochrony danych w konkretnym podmiocie są zwykle dodawane do „pakietów startowych" dla nowo zatrudnianych pracowników oraz wywieszane na wewnętrznej stronie intranetowej w zakładkach dotyczących ochrony danych w organizacji. Mogą być też wręczane osobom wraz z nadanym upoważnieniem do przetwarzania danych osobowych. Materiały te powinny być zwięzłe i czytelne dla pracowników.

Zwykle materiał, który przygotowuję, obejmuje 2, 3 strony. Oprócz wytłumaczenia prostym językiem podstawowych definicji z RODO skupiam się na podaniu najważniejszych informacji dotyczących wykonywania poszczególnych obowiązków, np. obowiązku informacyjnego (wskazuję, gdzie są wzory przeznaczonych do tego klauzul lub jak je ze mną –

jako IOD – konsultować itp.) czy obowiązku związanego z powierzaniem przetwarzania (gdzie jest wzór umowy, jak weryfikować potencjalnego procesora, jak konsultować treść umów itp.). Nie są to konkretne instrukcje, tylko odesłania do wewnętrznych instrukcji czy procedur w tym zakresie. W materiale zwracam też uwagę na podstawowe zasady zabezpieczania danych w postaci papierowej lub w dostępnym systemie informatycznym. Duży nacisk kładę na kwestię zgłaszania incydentów lub podejrzenia ich wystąpienia, które mogą prowadzić do naruszenia ochrony danych. Ważne, aby osoby wiedziały, jak i komu zgłaszać takie informacje.

Kolejną sprawą jest opracowanie odpowiednio dopasowanego programu szkoleń dla kadry kierowniczej i pracowników upoważnionych do przetwarzania danych. Zwykle szkolenia są dzielone na ogólne oraz dopasowane do potrzeb poszczególnych działów odpowiedzialnych za realizację zadań w ramach różnych procesów związanych z przetwarzaniem danych (np. kadry, sprzedaż, marketing, IT, obsługa klienta, administracja, recepcja itp.). Ogólne szkolenia mogą zawierać treści podobne do zawartych w materiałach informacyjnych, z dodanymi przykładami. Takie rozwiązanie osobiście realizuję w kilku podmiotach, gdzie mam świadomość trudności czytania ze zrozumieniem tego rodzaju materiałów. Poza tym od razu mogę wyjaśnić zapisane tam kwestie, a osoby w każdej chwili mogą powrócić do otrzymanego lub udostępnionego w intranecie skryptu.

Innym rodzajem szkoleń może być e-learning, zwykle z pytaniami sprawdzającymi. Na IOD spoczywa w tym wypadku przygotowanie odpowiedniego wsadu merytorycznego. Istotne jest uatrakcyjnienie takiego szkolenia od strony wizualnej. Pewne informacje można wyróżnić odpowiednimi oznaczeniami lub hasłami do zapamiętania. Warto skorzystać z programów graficznych, aby osiągnąć dobry efekt. Należy jednak pamiętać o czytelności treści. Nie powinno się też nadmiernie cytować wprost przepisów RODO. Szkolenia należy okresowo powtarzać i dostosowywać do potrzeb danej organizacji, np. uzupełniać o przykłady występujących naruszeń ochrony danych i wskazówki, jak ich unikać. Należy też zmieniać odpowiednio pytania sprawdzające, tak aby korygować problemy mogące pojawiać się przy przetwarzaniu i zabezpieczaniu danych.

Ważnym elementem realizacji obowiązków informacyjnych jest monitorowanie przez IOD zmian w prawie ochrony danych osobowych oraz pojawiających się rekomendacji i wytycznych organu nadzorczego i Europejskiej Rady Ochrony Danych. Informacje o zmianach w przepisach lub w praktyce realizacji obowiązków RODO powinny być niezwłocznie komunikowane kadrze kierowniczej i osobom upoważnionym do przetwarzania danych. Sprawdzianem tego zadania było wejście w życie 4.5.2019 r. WprowRODOU, zmieniającej ponad 160 przepisów w związku z zapewnieniem stosowania RODO. Wielu IOD nie poinformowało o tym fakcie, przez co naraziło się na zarzut nienależytego wypełniania zadań określonych w art. 39 ust. 1 lit. a RODO.

Ad 2. Drugim zadaniem wykonywanym na co dzień przez IOD jest doradzanie w zakresie realizacji obowiązków RODO w danej organizacji. To najważniejsze z zadań, które definiuje realną potrzebę czy konieczność wyznaczenia IOD przez administratora danych lub podmiot przetwarzający. Ta rola doradcza IOD jest niezbędna do zapewnienia przetwarzania danych zgodnie z RODO, jak również wykazywania zgodności przestrzegania obowiązków RODO. Aby podołać temu zadaniu, szczególnie w podmiotach, w których

jest realizowana duża liczba procesów przetwarzania danych, IOD powinien określić szczegółowe zasady dotyczące udzielania porad i odpowiedzi na pytania. Po pierwsze, należy wskazać specjalny adres e-mail lub numer telefonu, na które będą kierowane zapytania, a po drugie – najważniejsze – ustalić czas reakcji IOD na przesłane zapytania. Osoby zwracające się z problemami do IOD muszą mieć świadomość, że odpowiedź dotycząca złożonych problemów związanych z przetwarzaniem danych nie będzie udzielona od ręki, zwłaszcza jeżeli z danym tematem IOD nie był wcześniej zapoznany, pomimo obowiązku niezwłocznego włączania w takie sprawy. Istotne jest również ustalanie priorytetów w sytuacji, gdy wpływa dużo zapytań w tym samym czasie. Najważniejsze, aby informować pytających o przewidywanym czasie odpowiedzi oraz jej formie. Czasem wystarczy wskazówka lub drobna korekta np. klauzuli informacyjnej – nie ma potrzeby pisania długich opinii na każdy temat.

Na potrzeby realizacji konsultacji zalecam stworzenie rejestru konsultacji. Takie rejestry pomagają IOD w rozliczaniu się z tego zadania i zapobiegają umykaniu zapytań. Zakres doradzania może być różny. Obejmuje m.in. opiniowanie lub opracowywanie projektów dokumentów, np. klauzul informacyjnych, weryfikację umów powierzania przetwarzania danych i weryfikację podstaw prawnych przetwarzania danych oraz adekwatnych zakresów danych czy czasów ich retencji. Przy wykonywaniu tego zadania ważne jest monitorowanie liczby zapytań i problemów, dzięki czemu IOD może mieć dobre argumenty do wnioskowania do zarządu lub kierownictwa administratora o dodatkowe zasoby lub zewnętrzne wsparcie doradcze.

Ad 3. Trzecie z głównych zadań IOD – monitorowanie przestrzegania przepisów o ochronie danych oraz polityk ochrony danych wdrożonych u administratora lub podmiotu przetwarzającego – jest związane z przeprowadzaniem wewnętrznych audytów zgodności przetwarzania z przepisami RODO oraz krajowymi przepisami uzupełniającymi RODO. To zadanie wiąże się z wypełnianiem obowiązku wykazywania przestrzegania przepisów RODO przez administratora danych (zasada rozliczalności, o której mowa w art. 5 ust. 2 RODO) oraz zapewnieniem wykazywania zgodności działań z RODO, o którym mowa w art. 24 ust. 1 RODO. Mogą to być zarówno zaplanowane audyty okresowe, np. raz w roku, jak i audyty doraźne w odniesieniu do danego procesu przetwarzania danych, zwłaszcza w sytuacji wystąpienia lub podejrzenia naruszenia ochrony danych. Takie działania mogą być wykonywane przez IOD również wobec podmiotów przetwarzających, z którymi zawarte są umowy powierzenia przetwarzania danych. Wówczas zasady ich wykonywania powinny być określone w umowie powierzenia zgodnie z wymogiem art. 28 ust. 3 lit. h RODO.

Na potrzeby realizacji okresowych audytów IOD powinien przygotować ich plan oraz termin realizacji. W planie należy określić cel i zakres audytu oraz wskazać komórki organizacyjne objęte audytem. Audyt powinien być zakończony raportem zgodności z przepisami o ochronie danych oraz wewnętrznymi politykami ochrony danych. Inspektor może skorzystać ze swojego doświadczenia przy wykonywaniu sprawdzeń zgodności przetwarzania danych, które realizował wcześniej jako ABI. Zasady i tryb wykonywania sprawdzeń określone w starych przepisach wykonawczych, wydanych na potrzeby wyko-

nywania zadań ABI, mogą być tu dobrym wzorcem (zob. rozdział 2 nieobowiązującego już ZapPrzestrzPrzepR) – również dla osób, które wcześniej nie pełniły funkcji ABI.

1.5.2. Pozostałe zadania inspektora ochrony danych

Pozostałe zadania, które IOD ma obowiązek wykonywać w zależności od danej sytuacji, to:

1) doradzanie w zakresie wykonywania oceny skutków dla ochrony danych w odniesieniu do planowanych operacji ich przetwarzania oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
2) współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla tego organu, w tym w sytuacji zgłoszenia naruszenia ochrony danych zgodnie z art. 33 RODO oraz zgłoszenia potrzeby uprzednich konsultacji, o których mowa w art. 36 RODO.

Oprócz zadań wskazanych w art. 39 ust. 1 RODO inspektor ma obowiązek pełnienia punktu kontaktowego dla osób, których dane dotyczą, w sprawach związanych z przetwarzaniem ich danych osobowych oraz wykonywaniem przysługujących im praw, o czym mowa w art. 38 ust. 4 RODO.

Przepisy RODO dopuszczają również możliwość powierzenia IOD innych zadań, w tym związanych z realizacją obowiązków z nich wynikających, pod warunkiem że zadania te nie będą powodować konfliktu interesów (art. 38 ust. 6 RODO). Grupa Robocza Art. 29 w swoich wytycznych wskazała jako przykład możliwych do realizacji dodatkowych zadań IOD prowadzenie rejestrów czynności przetwarzania danych osobowych, o których mowa w art. 30 RODO[11]. Z praktyki wynika, że to właśnie zazwyczaj IOD opracowuje i prowadzi dokumentację dotyczącą przetwarzania danych, w tym wspomniane rejestry. Stąd to zadanie jest zwykle dodawane do zakresu obowiązków IOD.

1.5.2.1. Udział w prowadzeniu dokumentacji dotyczącej przetwarzania danych

Nadzór nad opracowaniem i aktualizowaniem dokumentacji przetwarzania danych osobowych to jedno z zadań, jakie realizowały osoby pełniące funkcję ABI w ramach wykonywania obowiązków zapewniania przestrzegania przepisów o ochronie danych osobowych u administratora. Stąd naturalne jest, że obecnie to zadanie zazwyczaj wykonuje IOD w odniesieniu do wymogów prowadzenia dokumentacji wynikającej z RODO. W RODO nie są określone szczegółowe rodzaje dokumentów, tak jak było w poprzednich przepisach o ochronie danych osobowych (rodzaj i zakres dokumentacji określały przepisy wykonawcze do OchrDanych97). Mowa jest o wdrożeniu przez administratora odpowiednich polityk ochrony danych jako jednego ze środków techniczno-organizacyjnych, jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania danych zgodnie z art. 24 ust. 1 i 2 RODO. Zatem to administrator decyduje, jaki rodzaj dokumentacji polityk będzie odpowiedni w jego przypadku. Należy jednak pamiętać, że środki techniczne i organizacyjne podejmowane w celu zapewnienia przetwarzania zgodnego z RODO powinny być dobrze opisane, tak aby można było wykazać ich stosowanie. W związku

[11] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych…, s. 19–20.

z tym polityka ochrony danych, jako główny dokument dotyczący ochrony danych w organizacji, powinna zawierać opis sposobu realizacji poszczególnych obowiązków RODO przez administratora danych.

Administrator danych może powierzyć IOD opracowanie dokumentacji jako dodatkowe zadanie na podstawie art. 38 ust. 6 RODO. Inspektor, opracowując politykę ochrony danych, określa w niej zasady przetwarzania danych osobowych, których realizację nadzoruje w ramach wykonywania zadań monitoringu przestrzegania przepisów o ochronie danych w organizacji administratora lub podmiotu przetwarzającego. W praktyce dokumentacja polityki ochrony danych składa się z kilku rodzajów dokumentów tworzonych w zależności od potrzeb, w tym:

1) polityki ochrony danych (głównego dokumentu opisującego zasady dotyczące przetwarzania danych osobowych przyjęte w organizacji w odniesieniu do realizacji wymogów określonych w art. 5 RODO),
2) instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych (opisującej zasady realizacji wymogów określonych w art. 33 i 34 RODO),
3) instrukcji realizacji praw osób, których dane dotyczą (opisującej zasady realizacji wymogów wskazanych w art. 15–22 RODO),
4) procedury szacowania ryzyka naruszenia praw lub wolności osób, których dane dotyczą, w tym oceny skutków dla ochrony danych (opisującej zasady realizacji wymagań określonych w art. 25, 32 i 35 RODO),
5) procedury dotyczącej nadawania upoważnień do przetwarzania danych (opisującej zasady realizacji wymogów określonych w art. 29 oraz art. 32 ust. 4 RODO),
6) procedury dotyczącej powierzania przetwarzania danych osobowych (opisującej zasady realizacji wymogów art. 28 RODO).

Oprócz koniecznych dokumentów, które określają zasady przetwarzania danych osobowych, należy prowadzić również dokumentację potwierdzającą realizację poszczególnych obowiązków określonych w RODO na potrzeby ich rozliczalności, w tym:

1) rejestry czynności przetwarzania danych osobowych – administratora oraz podmiotu przetwarzającego – prowadzone zgodnie z art. 30 RODO,
2) dokumentację dotyczącą naruszeń ochrony danych osobowych – prowadzoną zgodnie z art. 33 ust. 5 RODO,
3) dokumentację z przeprowadzonego szacowania ryzyka naruszenia praw lub wolności osób, których dane dotyczą, w tym plan postępowania z ryzykiem – na potrzeby wdrożenia odpowiednich środków technicznych i organizacyjnych: zabezpieczenia danych, o których mowa w art. 32 oraz 25 RODO,
4) dokumentację z przeprowadzonej oceny skutków dla ochrony danych, o której mowa w art. 35 ust. 7 RODO,
5) dokumentację potwierdzającą realizację żądań osób, których dane dotyczą – w odniesieniu do realizacji praw osób opisanych w art. 15–22 RODO,
6) dokumentację dotyczącą nadanych upoważnień do przetwarzania danych, w tym odebranych zobowiązań zachowania tajemnicy danych – w odniesieniu do realizacji wymogów zawartych w art. 32 ust. 4 oraz art. 28 ust. 3 lit. b RODO,

7) dokumentację z okresowych audytów zgodności przetwarzania danych z wymogami RODO – w odniesieniu do wymogów określonych w art. 24 ust. 1, art. 32 ust. 1 lit. d oraz art. 39 ust. 1 lit. b RODO.

Prowadzenie wyżej wskazanej dokumentacji potwierdzającej realizację wymogów RODO może być w pewnym zakresie powierzone IOD – zazwyczaj jest to prowadzenie rejestrów czynności przetwarzania danych oraz dokumentacji dotyczącej naruszeń ochrony danych – lub wynikać z realizacji jego głównych zadań, tak jak w przypadku prowadzenia audytów zgodności w ramach zadań związanych z monitorowaniem przestrzegania przepisów o ochronie danych osobowych. Zdarzają się jednak przypadki cedowania na IOD prowadzenia całości tego rodzaju dokumentacji. Nie jest to właściwe postępowanie, ponieważ może prowadzić do konfliktu interesów.

1.5.2.2. Udział w postępowaniu dotyczącym naruszenia ochrony danych

Zgodnie z wytycznymi Grupy Roboczej Art. 29 dotyczącymi zgłaszania naruszeń ochrony danych osobowych IOD powinien odgrywać kluczową rolę we wspieraniu administratora danych w zapobieganiu naruszeniom, przygotowaniu się na wypadek ich wystąpienia oraz w sytuacji wystąpienia takiego naruszenia. Zalecane jest, aby niezwłocznie informować IOD o wystąpieniu naruszenia oraz włączać go do procesu zarządzania taką sytuacją, w tym do zgłaszania informacji o naruszeniu do organu nadzorczego[12].

W ramach ustalania zasad postępowania w sytuacji naruszenia ochrony danych administrator danych powinien określić w nich udział IOD. Zazwyczaj IOD wchodzi w skład zespołu wyznaczanego do wyjaśniania sytuacji związanych z naruszeniami ochrony danych lub podejrzeniami zajścia takich sytuacji. Zdarzają się też rozwiązania, w których powoływany jest zespół ds. wyjaśniania incydentów związanych z bezpieczeństwem informacji, który konsultuje się z IOD jedynie w sytuacjach związanych z podejrzeniem naruszenia ochrony danych, na potrzeby potwierdzenia właściwego stwierdzenia zajścia takiego zdarzenia. Zespół, w którego skład zwykle wchodzi IOD, ma następujące zadania:

1) analiza zgłoszonych sytuacji podejrzenia naruszenia ochrony danych,
2) stwierdzenie naruszenia ochrony danych,
3) ocena poziomu ryzyka naruszenia praw osób, których dane dotyczą,
4) określenie konieczności zgłaszania zawiadomienia o naruszeniu ochrony danych do Prezesa UODO,
5) określenie konieczności poinformowania osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych,
6) podejmowanie działań zaradczych,
7) dokumentowanie naruszeń ochrony danych osobowych.

[12] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP250rev.01), przyjęte 3.10.2017 r., ostatnio zmienione i przyjęte 6.2.2018 r., https://uodo.gov.pl/pl/10/12 (dostęp: 8.11.2019 r.), s. 32–33.

Przejdź do księgarni