Artur Piechocki
Radca prawny w kancelarii APLaw Artur Piechocki.

Daniel Siciński
Aplikant radcowski w kancelarii APLaw Artur Piechocki.

Pozycja i zadania ABI w świetle reformy ochrony danych osobowych

Do wejścia w życie nowego europejskiego rozporządzenia w sprawie ochrony danych osobowych[1] (rozporządzenie, RODO) pozostał już niecały rok. Stosowane bezpośrednio w każdym kraju Unii Europejskiej od 25 maja 2018 roku, nowe rozporządzenie, wprowadzi duże zmiany również w polskim systemie ochrony danych osobowych, zastępując obecnie obowiązujące przepisy w tym zakresie. Celem niniejszego opracowania jest przegląd najważniejszych zmian, jakie RODO wprowadzi w obszarze zadań realizowanych obecnie przez administratorów bezpieczeństwa informacji (ABI).

Przepisy dotyczące ABI są obecnie zawarte przede wszystkim w art. 36a i nast. ustawy o ochronie danych osobowych[2] (uodo), a także w rozporządzeniach wykonawczych wydanych na jej podstawie. Od wejścia w życie RODO, status i zadania ABI będą regulowane przede wszystkim przepisami zawartymi w art. 37-39 rozporządzenia, a jedynie w uzupełniającym zakresie projektowaną obecnie nową ustawą o ochronie danych osobowych. Ze względu na ogólne sformułowanie obowiązków inspektorów ochrony danych[3] (IOD), dla praktyki stosowania nowych przepisów istotne znaczenie będą miały również wytyczne Grupy Roboczej Artykułu 29[4] (GR29), organów nadzorczych w innych krajach europejskich, w tym wytyczne GIODO[5].

Wprowadzone przez RODO nowe rozwiązania, wpłyną na pozycję i zakres obowiązków realizowanych przez ABI, przy czym nie będzie to zmiana rewolucyjna, gdyż wiele z tych rozwiązań funkcjonuje w polskich przepisach już w 2015 roku[6]. Nowe podejście do ochrony danych, oparte na zasadzie rozliczalności i konieczności uwzględniania ryzyka przetwarzania dla praw i wolności osób, wymaga aktywnego wsparcia administratorów danych osobowych (ADO) i podmiotów przetwarzających dane w ich imieniu przez osoby o dużej wiedzy i umiejętnościach, które będą w stanie zapewnić zgodność procesów przetwarzania z nowymi przepisami. Z tego względu obecna pozycja ABI ulegnie wzmocnieniu, a funkcjonująca już obecnie zasada jego niezależności będzie zapewniona przez konkretne instrumenty. Istotną zmianą będzie również wprowadzenie obowiązku powołania IOD w określonych przypadkach, doprecyzowanie wymagań, jakie powinny spełniać osoby pełniące tę funkcję, a także zmiany w zakresie zadań wykonywanych przez obecnych ABI.

Powołanie IOD

Obecnie obowiązujące przepisy, pozostawiają administratorom danych możliwość wyboru w zakresie powoływania ABI. RODO przewiduje zasadniczą zmianę w tym zakresie, poprzez **obowiązek powołania IOD** w przypadkach, gdy:

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej jako: ogólne rozporządzenie o ochronie danych, RODO).

[2] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2016, poz. 922).

[3] Taką nazwę RODO przyjmuje dla obecnych ABI.

[4] Po wejściu w życie RODO funkcje tego organu pełnić będzie Europejska Rada Ochrony Danych.

[5] Od dnia wejścia w życie nowej ustawy o ochronie danych osobowych określany jako Prezes Urzędu Ochrony Danych Osobowych.

[6] Nowelizacją UODO wprowadzona w życie ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz.U. z 2014, poz. 1662).

1) przetwarzania dokonuje **organ lub podmiot publiczny**, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości,

2) **główna działalność administratora lub podmiotu przetwarzającego, polega na operacjach przetwarzania**, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania na dużą skalę osób, których dane dotyczą,

3) **główna działalność administratora lub podmiotu przetwarzającego, polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych** oraz danych osobowych dotyczących **wyroków skazujących i naruszeń prawa.**

Co istotne, rozporządzenie wprost stwierdza, że IOD może być powołany nie tylko przez ADO, jak to jest na gruncie obecnych przepisów, ale także przez podmioty przetwarzające. Nowością będzie również możliwość powołania jednego IOD przez grupę przedsiębiorców (np. grupę kapitałową) lub przez kilka organów czy podmiotów publicznych (np. związek gmin). W przypadku takiego rozwiązania, IOD będzie musiał był dostępny w takim samym zakresie dla każdego z administratorów, jego pracowników, a także osób, których dane są przetwarzane. W przypadku międzynarodowych grup kapitałowych istotne będzie zapewnienie, aby IOD mógł komunikować się z podmiotami danych oraz organami nadzorczymi z różnych krajów w ich języku ojczystym. RODO przewiduje także możliwość powołania jednego IOD przez zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających, dając IOD uprawnienie do reprezentowania takich podmiotów.

Obecnie administratorzy nie mają obowiązku samodzielnego udostępniania danych kontaktowych ABI, poza obowiązkiem zgłoszenia GIODO faktu jego powołania i odwołania zgodnie ze sformalizowaną procedurą opisaną w art. 46b i nast. uodo. Stosownie do nowych przepisów, uwzględniając również wytyczne GR29, dane kontaktowe IOD powinny być udostępnione nie tylko organowi nadzorczemu, ale również osobom, których dane są przetwarzane oraz wewnątrz organizacji ADO lub podmiotu przetwarzającego. Jest to istotne w świetle nowego założenia, zgodnie z którym IOD ma pełnić funkcję punktu kontaktowego oraz pośrednika między organem nadzorczym, ADO (przetwarzającym) oraz podmiotami danych. Jeśli chodzi o zakres danych przekazywanych Prezesowi Urzędu, to jest on znacznie węższy, niż ten przewidziany w art. 46b ust. 2 uodo i będzie ograniczał

się do wskazania imienia i nazwiska IOD wraz z adresem jego poczty elektronicznej oraz numerem telefonu. Projekt nowej ustawy o ochronie danych osobowych[7] przewiduje, iż ADO lub podmiot przetwarzający, powinien informować Prezesa Urzędu o jego wyznaczeniu oraz każdej zmianie w tym zakresie w terminie 14 dni od dnia takiej zmiany, przy czym będzie to mogło następować zarówno w formie papierowej, jak i elektronicznej.

Wymagania podmiotowe wobec IOD

Istotną zmianą wprowadzoną przez nowe przepisy, będzie możliwość wykonywania funkcji IOD nie tylko przez osoby fizyczne, jak to ma miejsce obecnie, ale także osoby prawne i inne jednostki organizacyjne. Wytyczne GR29[8] doprecyzowują, iż zadania IOD będą mogły być realizowane na podstawie umowy o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem spoza organizacji administratora lub podmiotu przetwarzającego, a także przez grupę osób bezpośrednio podległą IOD. W takich przypadkach istotny będzie jednak wyraźny podział zadań realizowanych przez każdą z takich osób, a także wyznaczenie jednej osoby kontaktowej dla podmiotów danych.

Tak jak obecnie, IOD będzie musiał wykazać się posiadaniem wiedzy i doświadczenia z obszaru danych osobowych, przy czym rozporządzenie oraz wytyczne GR29 wymóg ten znacznie doprecyzowują. Ocena kwalifikacji IOD będzie dokonywana przez pryzmat charakteru wykonywanych operacji przetwarzania, rodzaju oraz ilości wykorzystywanych danych oraz ochrony koniecznej do zapewnienia przetwarzanym danym. Przykładowo, wyższych kwalifikacji będzie się wymagało od IOD mających czuwać nad złożonymi procesami przetwarzania w systemach informatycznych dużej ilości danych osobowych, w szczególności wrażliwych, w tym jeśli byłoby to związane z transgranicznym przekazywaniem danych. Zawsze jednak IOD powinien wykazywać się wiedzą teoretyczną i praktyczną z obszaru przepisów europejskich oraz krajowych, dotyczących przetwarzania danych osobowych. IOD powinien również znać procesy przetwarzania w organizacji, wykorzystywane w tym celu systemy informatyczne, zagrożenia, zabezpieczenia i potrzeby administratora (przetwarzającego) w tym zakresie, w tym także profil ich działalności i związane z nim wymogi prawne. W kontekście realizacji zadań IOD przez jednostki organizacyjne, wskazane kwalifikacje podmiotowe będą musiały spełniać wszystkie osoby wykonujące w ramach tej jednostki funkcje przewidziane dla IOD.

Status IOD w organizacji

RODO utrzyma obowiązujący obecnie wymóg wyodrębnienia organizacyjnego IOD i podporządkowania go bezpośrednio kierownictwu administratora (podmiotu przetwarzającego), co ma zapewnić możliwość niezależnego i bezpośredniego zgłaszania mu uwag związanych z przetwarzaniem danych osobowych w organizacji. Nowością będzie wyraźne sformułowanie obowiązku zapewnienia udziału IOD we wszystkich sprawach związanych z ochroną danych osobowych, wspierania go w realizacji zadań, w szczególności poprzez zapewnienie w tym celu niezbędnych zasobów finansowych i organizacyjnych oraz dostępu do danych osobowych i operacji przetwarzania. IOD będzie mógł również domagać się od administratora (przetwarzającego) umożliwienia utrzymania swojej wiedzy fachowej, a także zapewnienia na ten cel środków finansowych.

Szczególnie istotną zmianą będzie wprowadzenie przepisów wprost zakazujących wydawania IOD jakichkolwiek instrukcji, dotyczących wykonywania przez niego zadań. Nie będzie więc dopuszczalne sugerowanie IOD, w jaki sposób ma załatwić określony wniosek podmiotu danych, interpretować przepisy w zakresu ochrony danych czy też jak ma prowadzić audyt przestrzegania przepisów. Powiązany z tą gwarancją niezależności będzie również wyraźny zakaz dyskryminacyjnego traktowania IOD wynikającego z wykonywania przez niego swoich zadań. W szczególności, administrator (przetwarzający) nie będzie mógł z tego powodu np. obniżyć mu wynagrodzenia, odmówić awansu lub dostępu do szkoleń, ukarać go w jakikolwiek inny sposób lub wypowiedzieć umowę, na podstawie której IOD wykonuje swoją pracę.

Podobnie jak obecnie obowiązujące przepisy, rozporządzenie formułuje wymóg zapewnienia przez administratora lub podmiot przetwarzający, aby IOD wykonywał inne obowiązki jedynie w takim zakresie, w jakim nie będą uniemożliwiały mu wykonywania zadań związanych z ochroną danych. Chodzi tu zarówno o zagwarantowanie odpowiednich warunków czasowych i organizacyjnych na realizację tych zadań, jak również przeciwdziałanie powstawaniu konfliktu interesów. Mogłoby do niego dojść przykładowo wówczas, gdyby funkcję IOD miał realizować kierownik jednego z działów w organizacji, przez co w istocie musiałby on nadzorować przestrzeganie wymogów ochrony danych przez siebie i swoich podwładnych.

Zadania realizowane przez IOD

Część zadań realizowanych przez IOD ulegnie zmianie w porówna-

[7] Dostępny pod adresem: https://mc.gov.pl/projekty/nowe-prawo-ochrony-danych-osobowych/projekt-przepisow (dostęp: 19 sierpnia 2017 r.).

[8] Polska wersja wytycznych dostępna pod adresem: http://giodo.gov.pl/pl/1520285/9740 (dostęp: 19 sierpnia 2017 r.).

niu do tych wykonywanych obecnie przez ABI, przy czym IOD nadal będzie przede wszystkim wspierać administratorów i podmioty przetwarzające w wykonywaniu przez nich obowiązków. W dalszym ciągu IOD będzie zobowiązany do monitorowania przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych polityk, w tym poprzez prowadzenie audytów, a także do informowania osób przetwarzających dane o istniejących w tym zakresie wymogach, w szczególności poprzez realizację regularnych szkoleń. Inaczej będzie wyglądała współpraca z Prezesem Urzędu, który nie będzie już mógł zwrócić się do IOD z wnioskiem o przeprowadzenie sprawdzenia, ale będzie mógł kontaktować się z nim w ramach procedury uprzedniej konsultacji oceny skutków przetwarzania (o czym niżej), a także w innych sprawach. RODO wyraźnie wskazuje, iż IOD ma również udzielać pomocy i wyjaśnień w razie wystąpienia z takim wnioskiem przez osoby, których dane są przetwarzane, w zakresie realizacji przez nie uprawnień wynikających z przepisów.

Ponieważ RODO nakłada na administratorów i podmioty przetwarzające wiele nowych obowiązków, IOD powinien być przygotowany do doradzania oraz monitorowania przestrzegania przepisów również w tym zakresie. Chodzi przykładowo o nowe uprawnienia podmiotów danych, takie jak prawo „do bycia zapomnianym" lub prawo do przenoszenia danych, obowiązek zgłaszania naruszeń ochrony danych osobowych, realizację bardziej rozbudowanych niż dotychczas obowiązków informacyjnych, konieczność uwzględniania prywatności w fazie projektowania oraz w ustawieniach domyślnych itd.

Rozporządzenie nakłada na IOD nowy obowiązek w postaci konsultowania się z administratorem w przypadku sporządzania przez niego oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Jest to nowe narzędzie przewidziane przez RODO, które ma umożliwić administratorowi ocenę ryzyka związanego z określonymi procesami przetwarzania oraz ich ograniczenie poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych. IDO powinien brać aktywny udział w sporządzaniu oceny przez administratora, przede wszystkim poprzez doradzanie w stosunku do jakich procesów zachodzi konieczność jej przeprowadzenia, jaką metodologię należy przyjąć, czy ocena ma by wykonana przez podmiot zewnętrzny, czy w ramach organizacji, czy ocena została przeprowadzona prawidłowo oraz jakie techniczne lub organizacyjne środki należy wdrożyć w celu minimalizacji ustalonych w jej toku ryzyk. W przypadkach, w których ocena potwierdzi wysokie ryzyko dla ochrony danych osobowych wymagające zastosowania środków minimalizujących zagrożenie, administrator będzie zobowiązany przeprowadzić konsultacje z Prezesem Urzędu, a IOD będzie w nich aktywnie uczestniczył, pełniąc rolę punktu kontaktowego dla organu nadzorczego.

W przypadkach opisanych w art. 30 ust. 5 RODO na administratorów i podmioty przetwarzające został nałożony obowiązek prowadzenia **rejestru czynności przetwarzania**, który będzie zbliżony pod kątem zawartości do prowadzonych obecnie przez ABI rejestrów zbiorów danych. Nie jest to zatem obowiązek IOD, jednak w praktyce to ten podmiot będzie posiadał niezbędną wiedzę i doświadczenie w zakresie opracowywania tego typu rejestru, a ponadto jego prowadzenie powinno w istotnym stopniu ułatwić mu wykonywanie innych zadań wynikających z przepisów. Z tych względów wydaje się, iż dopuszczalne i wskazane byłoby powierzanie przez administratorów i podmioty przetwarzające prowadzenia tych rejestrów przez IOD.

Z pewnością dużą zmianą dla praktyki przyszłych IOD będzie brak sformalizowanych wymogów w zakresie sporządzania i treści **polityki bezpieczeństwa** oraz **instrukcji zarządzania systemem informatycznym**, brak obowiązku prowadzenia rejestrów zbiorów danych w obecnym kształcie, czy też obowiązku wykonywania sprawdzeń i sprawozdań dotyczących zgodności przetwarzania danych osobowych z przepisami. Z drugiej strony należy pamiętać, iż rozporządzenie celowo unika określania konkretnych narzędzi (z wyjątkiem wspomnianej oceny skutków przetwarzania czy rejestru czynności przetwarzania), które powinny być wykorzystywane dla zapewnienia zgodności przetwarzania danych z przepisami, wprowadzając za to zasadę podejścia opartego na ryzyku. Oznacza to konieczność uwzględnienia istniejącego i potencjalnego ryzyka dla ochrony danych osobowych, nadanie priorytetu operacjom przetwarzania wiążącym się z większym ryzykiem oraz wdrożenia takich środków, które w opinii ADO lub podmiotu przetwarzającego będą odpowiednie dla ich ograniczenia.

Równocześnie rozporządzenie wprowadza **zasadę rozliczalności** (art. 5 ust. 2 RODO), która wiąże się z obowiązkiem sporządzenia dokumentacji umożliwiającej wykazanie przed organem nadzorczym, że takie środki lub procedury zostały wdrożone w celu zabezpieczenia danych osobowych. Dlatego też art. 24 ust. 2 RODO nakłada na ADO obowiązek przyjęcia odpowiednich polityk ochrony danych, nie precyzując przy tym, jaka ma być ich forma i treść. Zatem to administrator danych będzie musiał określić wspólnie z IOD (art.

38 ust. 1 RODO), jaki system zarządzania ochroną danych powinien zostać przyjęty w organizacji ze względu na charakter procesów przetwarzania i ryzyka z nimi związanego.

Kary pieniężne oraz okres przejściowy

Przestrzeganie nowych przepisów dotyczących powoływania, statusu oraz zadań IOD powinno być szczególnie istotne dla administratorów danych oraz podmiotów przetwarzających ze względu na przewidziane w RODO kary pieniężne w razie ich naruszenia, w tym także w przypadku nienależytego wykonywania zadań przez IOD. W takim przypadku rozporządzenie przewiduje możliwość nałożenia na te podmioty kary sięgającej do 10 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Z tego względu w projektowanej ustawie o ochronie danych osobowych przewidywane jest rozwiązanie, które umożliwi obecnym ABI dokonanie świadomego wyboru, czy będą chcieli dalej wykonywać swoje funkcje jako IOD. Projekt przewiduje bowiem, że osoby wykonujące funkcję ABI na dzień rozpoczęcia stosowania rozporządzenia (25 maja 2018 r.) będą pełniły funkcję IOD w sposób tymczasowy do dnia 1 września 2018 r. W razie woli dalszego zachowania statusu IOD, konieczne będzie dokonanie zgłoszenia danych kontaktowych Prezesowi Urzędu. Brak aktywności w tym zakresie będzie skutkował tym, iż po dacie 1 września 2018 r. z mocy prawa osoby takie przestaną pełnić funkcję IOD. Nic nie będzie również stało na przeszkodzie, aby administratorzy bezpieczeństwa informacji, którzy nie będą chcieli od przyszłego roku pełnić funkcji IOD, zgłosili ADO swoją rezygnację jeszcze przed dniem 25 maja 2018 r, co będzie zobowiązywało ADO do zgłoszenia tego faktu GIODO.

Podsumowanie najważniejszych zmian wprowadzonych przez RODO w odniesieniu do statusu i zadań ABI[1]

Obecnie obowiązujące przepisy	RODO
Brak obowiązku powołania ABI.	Obowiązek powołania IOD w określonych przypadkach.
Funkcję ABI może pełnić tylko osoba fizyczna powołana przez administratora danych.	Funkcję IOD może pełnić także jednostka organizacyjna powołana zarówno przez ADO, jak i podmiot przetwarzający.
Brak przepisów o wspólnym ABI.	Możliwość powołania jednego IOD dla grupy przedsiębiorców oraz podmiotów publicznych.
ADO zgłasza fakt powołania i odwołania ABI organowi nadzorczemu, przekazując szeroki zakres danych.	ADO przekazuje organowi nadzorczemu, swoim pracownikom i podmiotom danych wyłącznie dane kontaktowe IOD oraz zmiany w tym zakresie.
ABI ma mieć odpowiednią wiedzę z zakresu ochrony danych osobowych.	Wiedza i doświadczenie IOD powinny być dostosowane do procesów przetwarzania, specyfiki działalności i potrzeb ADO.
Ogólny wymóg niezależności ABI oraz konieczności zapewnienia środków dla realizacji zadań.	Zakaz wydawania instrukcji oraz odwoływania IOD w związku z wykonywaniem zadań; obowiązek wspierania IOD, zapewnienia dostępu do danych i procesów oraz środków do utrzymywania wiedzy.
Zadania ABI obejmują sprawdzanie przestrzegania oraz informowanie o przepisach, nadzorowanie opracowywania dokumentacji, prowadzenie rejestrów zbiorów danych oraz dokonywanie sprawdzeń i sporządzanie sprawozdań.	Poza monitorowaniem przestrzegania i doradzaniem w zakresie nowych przepisów, IOD uczestniczy w sporządzaniu oceny skutków przetwarzania, prowadzi audyty i szkolenia, współpracuje i pełni funkcję punktu kontaktowego z Prezesem Urzędu oraz podmiotami danych.
Przepisy określają, jaka dokumentacja ma być prowadzona przez ADO i podmiot przetwarzający.	Obowiązek sporządzania konkretnej dokumentacji zastępuje zasada rozliczalności oraz podejścia opartego na ryzyku.
Brak kar finansowych za nieprzestrzeganie przepisów o ABI.	Kary finansowe w przypadku naruszenia przepisów o IOD.

[1] Opracowanie własne APLaw.