Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych

dr Edyta Bielak-Jomaa
Piotr Drobek
Dorota Krajewska-Kekusz
Monika Młotkiewicz
dr Maciej Kawecki
Tomasz Soczyński
dr inż. Andrzej Kaczmarek
Katarzyna Hildebrandt

Biuro Generalnego Inspektora Ochrony Danych Osobowych
Warszawa 2016

Autorzy
dr Edyta Bielak-Jomaa
Piotr Drobek
Dorota Krajewska-Kekusz
Monika Młotkiewicz
dr Maciej Kawecki
Tomasz Soczyński
dr inż. Andrzej Kaczmarek
Katarzyna Hildebrandt

Redakcja
Martyna Wilk

Korekta
Urszula Włodarska

Skład i łamanie
Marcin Szewczyk

Projekt okładki
Dagmara Jagodzińska

Produkcja
PRESSCOM Sp. z o.o.
ul. T. Kościuszki 29, 50-011 Wrocław
tel. 71 797 28 46, faks 71 797 28 16
e-mail: biuro@presscom.pl

Wydawca
Biuro Generalnego Inspektora
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
tel. 22 531 03 00, faks 22 531 03 01
e-mail: kancelaria@giodo.gov.pl

ISBN 978-83-913680-4-6

Spis treści

Wprowadzenie

W dobie globalizacji i rozwoju nowoczesnych technologii o pozycji podmiotów działających w różnych sektorach i branżach coraz częściej decydują dane. Szczególne znaczenie mają dane osobowe, które odgrywają coraz bardziej znaczącą rolę w tworzeniu i rozwijaniu nowych, innowacyjnych usług oraz przekształcaniu gospodarki w system ekonomiczny oparty na danych. Te zmiany są z jednej strony bodźcem do powstawania nowych miejsc pracy i wzrostu gospodarczego, z drugiej zaś niosą ze sobą nowe wyzwania i zagrożenia dla prywatności w związku z gromadzeniem i przetwarzaniem danych osobowych. Z tego m.in. powodu zapewnienie profesjonalnej obsługi procesów przetwarzania danych w organizacjach nabiera coraz większego znaczenia.

Jedną z głównych ról w tym zakresie mają do odegrania obecni administratorzy bezpieczeństwa informacji (ABI), a w przyszłości – inspektorzy ochrony danych. To oni mają w sposób profesjonalny działać na rzecz zapewnienia bezpieczeństwa danych osobowych w obrocie gospodarczym, stając się w ten sposób gwarantem właściwego, zgodnego z prawem przetwarzania danych osobowych.

Obecnie podstawowe zadania ABI są zdefiniowane w art. 36a ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. DzU z 2016 r. poz. 922; uodo), a ich realizacja wymaga posiadania przez ABI wiedzy z bardzo różnych dziedzin. Oprócz znajomości przepisów prawa o ochronie danych osobowych i orzecznictwa w tym zakresie powinni mieć oni wiedzę dotyczącą także: funkcjonowania systemów teleinformatycznych, metodologii prowadzenia kontroli i opracowywania specjalistycznej dokumentacji. Bardzo istotna w pracy ABI jest również umiejętność współpracy z ludźmi, gdyż do ich zadań należy m.in. przeprowadzanie szkoleń dla przedstawicieli zatrudniającej ich instytucji oraz przeprowadzanie konsultacji zarówno wewnętrznych, jak i z jednostkami zewnętrznymi.

W podobny sposób rola ABI ujęta została w unijnym rozporządzeniu ogólnym o ochronie danych (rodo), które bezpośrednio zacznie być stosowane od 25 maja 2018 r. Również ono fachową wiedzę uznaje za niezbędny warunek umożliwiający skuteczne wykonywanie funkcji inspektora ochrony danych (tak obecnego ABI nazywa ten dokument). Biorąc jednak pod uwagę fakt, że rozporządzenie to wprowadza istotne zmiany w systemie ochrony danych osobowych, czyniąc administratora danych podmiotem w większym niż dotąd stopniu odpowiedzialnym za zgodne z prawem przetwarzanie danych osobowych, to automatycznie rola i zadania wpierającego go w tym inspektora ochrony danych ulegną znacznej modyfikacji.

Celem niniejszej publikacji – przygotowanej przez ekspertów z Biura GIODO – jest przedstawienie, jak w świetle ogólnego rozporządzenia o ochronie danych i nowych zadań nałożonych na administratorów danych kształtować się będzie wykonywanie obowiązków inspektora ochrony danych. Generalny Inspektor Ochrony Danych Osobowych (GIODO) ma bowiem świadomość, że **fachowa wiedza inspektorów ochrony danych, przekładająca się na konkretne umiejętności praktyczne, jest fundamentem, na którym zbudować można w danej organizacji cały system skutecznej ochrony danych osobowych.**

dr Edyta Bielak-Jomaa, Generalny Inspektor Ochrony Danych Osobowych

Rozdział I
Istota unijnej reformy prawa ochrony danych osobowych – zmiana podejścia do ochrony danych osobowych

27 kwietnia 2016 r., w efekcie kilkuletnich prac legislacyjnych w UE, ostatecznie został przyjęty pakiet legislacyjny reformujący unijne prawo ochrony danych osobowych, który obejmuje dwa akty prawne:

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (DzUrz L nr 119 z 4.05.2016 r., s. 1; rodo) oraz
- dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (DzUrz L nr 119 z 4.05.2016 r., s. 89).

Obecna reforma następuje po ponad 20 latach od uchwalenia dyrektywy 95/46/WE, która obecnie jest podstawowym aktem prawnym regulującym kwestie ochrony danych osobowych w UE. W związku z tym można z dużym stopniem prawdopodobieństwa założyć, że oba nowo przyjęte akty prawne będą określały ramy ochrony danych osobowych przez najbliższe kilkadziesiąt lat. Niewątpliwie oba są ze sobą powiązane i dopiero w połączeniu zapewniają wprowadzenie kompleksowego systemu ochrony danych osobowych. Niemniej ze względu na zakres zastosowania i swój charakter prawny podstawowe znaczenie dla większości administratorów danych i podmiotów przetwarzających ma rodo.

Przyjęcie rodo oznacza więc, że docelowo kwestie ochrony danych osobowych w swojej zasadniczej części będą uregulowane w jednym akcie

prawnym obowiązującym w całej Unii Europejskiej, a nie tak, jak jest obecnie, czyli w 28 krajowych ustawach o ochronie danych osobowych, niejednokrotnie różniących się między sobą. Nie oznacza to jednak, że rodo całkowicie zastąpi krajowe ustawy o ochronie danych osobowych. Ustawodawca unijny przewiduje bowiem pewien obszar dla regulacji krajowych. Można je podzielić na cztery grupy. Pierwsza dotyczy spraw, co do których rodo wymaga przyjęcia przepisów krajowych. Dla przykładu: chodzi tutaj o konieczność ustanowienia niezależnego organu nadzorczego oraz zapewnienia mu odpowiednich środków do właściwego działania. Druga grupa dotyczy spraw, w których ustawodawca krajowy ma możliwość uregulowania odmiennie, choć w określonych ramach, kwestii wprost przewidzianych w rodo. Przykładem takiego rozwiązania jest umożliwienie państwom członkowskim obniżenia wieku dziecka, od którego może ono samodzielnie wyrazić zgodę na przetwarzanie danych w przypadku usług społeczeństwa informacyjnego. Rodo określa ten wiek na 16 lat. Jednak dopuszczając jego ograniczenie, wyraźnie zastrzega, że nie może on być niższy niż 13 lat. Trzecia grupa dopuszcza doprecyzowanie przez ustawodawcę krajowego określonych w nich kwestii. Wreszcie czwarta grupa dotyczy możliwości wprowadzenia przez ustawodawcę krajowego ograniczeń lub wyłączeń praw zagwarantowanych przez rodo po spełnieniu warunków w nim określonych.

Z polskiej perspektywy dużą nowością jest zwiększenie roli niewiążących wytycznych i wskazówek wydawanych zarówno na poziomie europejskim przez nowo powołaną Europejską Radę Ochrony Danych (która zastąpi obecnie funkcjonującą Grupę Roboczą Art. 29 ds. ochrony danych osobowych), jak i na poziomie krajowym przez organy nadzorcze, w tym Generalnego Inspektora Ochrony Danych Osobowych. Takie wytyczne i wskazówki będą miały bardzo duże znaczenie praktyczne dla administratorów danych i podmiotów przetwarzających, gdyż rodo określa ich obowiązki stosunkowo ogólnie, aby zapewnić im większą elastyczność w sposobie ich realizacji. Jednocześnie w większości sytuacji ustawodawca krajowy nie może uzupełnić lub doprecyzować tych obowiązków w przepisach krajowych.

Rodo weszło w życie 25 maja 2016 r., lecz jego stosowanie rozpocznie się dopiero od 25 maja 2018 r. Okres między tymi datami ma służyć dostosowaniu przepisów krajowych do nowych postanowień unijnych, a także umożliwić administratorom danych i podmiotom przetwarzającym, czyli działającym na zlecenie administratora, przygotowanie się do realizacji nowych obowiązków. W świetle motywu 171 preambuły rodo wszystkie toczące się wcześniej operacje przetwarzania danych muszą być dostosowane do nowych wymogów tak, aby już 25 maja 2018 r. móc zapewnić ich zgodność z przepisami rodo.

Z tego względu administratorzy danych oraz podmioty przetwarzające nie mogą czekać z przygotowaniami do zapewnienia zgodności z nowymi przepisami unijnymi do maja 2018 r., lecz powinni rozpocząć prace w tym zakresie dużo wcześniej. W miarę zbliżania się terminu rozpoczęcia stosowania rodo będą pojawiały się opinie i wytyczne przygotowane przez Grupę Roboczą Art. 29, m.in. w zakresie określenia pojęcia głównej jednostki organizacyjnej, statusu i kompetencji inspektora ochrony danych, a także rozumienia pojęcia operacji skutkujących wysokim ryzykiem dla praw i wolności osób, których dane dotyczą. Jednocześnie należy oczekiwać przyjęcia co najmniej nowej ustawy o ochronie danych osobowych, tak aby jej przepisy w uzupełnieniu rodo mogły być stosowane już od 25 maja 2018 r. Do tego czasu nadal należy przestrzegać obecnie obowiązujących przepisów o ochronie danych osobowych.

Dostosowanie zasad przetwarzania danych do aktualnego stanu wiedzy technologicznej

Jednym z celów przyświecających projektodawcom rodo było zapewnienie skuteczności ochrony danych osobowych w zmieniających się środowiskach: technologicznym, organizacyjnym i gospodarczym. Od czasu przyjęcia w 1995 r. dyrektywy 95/46/WE radykalnie zmieniły się metody przetwarzania danych osobowych, a tym samym pojawiły się nowe wyzwania związane ze skutecznym zapewnieniem ich odpowiedniej ochrony. Generowanie danych w postaci cyfrowej oraz zwiększające się możliwości ich wykorzystywania, które jeszcze kilka lat temu

nie były dostępne, zrodziły potrzebę zmiany modelu regulacji ochrony danych osobowych. Jednak nie oznacza to konieczności radykalnej zmiany podstawowych zasad ochrony danych osobowych, które wymagają zachowania. Należało jedynie je zmodyfikować oraz wprowadzić nowe instytucje odpowiadające na nowe problemy związane z przetwarzaniem danych osobowych w internecie.

Rodo zostało zbudowane na dotychczasowym dorobku legislacyjnym i orzeczniczym rozwijanym przez ostatnie 40 lat w Europie. Skoncentrowanie się na podstawowych zasadach ochrony danych osobowych oraz odejście od istniejących wcześniej obowiązków o charakterze notyfikacyjno-rejestracyjnym spowodowało zmianę modelu ochrony danych osobowych. Ten nowy ma na celu przeniesienie głównych zasad na poziom praktycznych rozwiązań i procedur oraz zapewnienie ich realnego przestrzegania.

Podstawowe zasady przetwarzania danych wg art. 5 rodo

- zasady legalności (zgodności z prawem), rzetelności i przejrzystości, zgodnie z którymi dane powinny być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- zasada ograniczenia celu, w myśl której dane powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami;
- zasada minimalizacji danych, zgodnie z którą dane powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
- zasada prawidłowości (poprawności), w myśl której dane mają być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- zasada ograniczenia przechowywania, zgodnie z którą dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane

dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy;
- zasada zapewnienia bezpieczeństwa danych, w tym ich integralności i poufności, zgodnie z którą dane muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Rodo w swoich założeniach ma być neutralne technologicznie. Jednocześnie jego postanowienia wprowadzają szczególne instrumenty prawne i mechanizmy odnoszące się do specyfiki gospodarki cyfrowej. Pojawiają się więc nowe lub zdefiniowane na nowo prawa, takie jak: prawo do usunięcia danych i prawo do zapomnienia oraz prawo do przenoszalności danych. Ponadto wprowadzono koncepcje, które dotąd były jedynie postulatami o charakterze teoretycznym, m.in.: zapewnienie ochrony danych na etapie projektowania, domyślna ochrona danych i zgłaszanie naruszeń ochrony danych osobowych. Zmodyfikowano również dotychczasowe zasady dotyczące automatycznego podejmowania decyzji opartych przede wszystkim na profilowaniu. Odniesienia do środowiska cyfrowego odnajdziemy również w modyfikacjach dotychczasowych definicji (np. pojęcie danych osobowych) i w zupełnie nowych definicjach wprowadzonych w rodo.

Bardzo ważną koncepcją, która przenika przepisy rodo, jest tzw. podejście oparte na ryzyku. Ryzyko (często stopniowane) naruszenia praw i wolności osób, których dane dotyczą, na gruncie rodo staje się jednym z kluczowych pojęć. Administrator danych oraz w różnym zakresie podmiot przetwarzający muszą brać pod uwagę istniejące i potencjalne ryzyka dla ochrony danych osobowych po to, by zastosować odpowiednie do nich środki bezpieczeństwa. Takie podejście umożliwia skoncentrowanie się na sytuacjach najwyższego ryzyka, przy jednoczesnym zachowaniu odpowiedniego poziomu ochrony, gdy

to ryzyko jest niskie i nie wymaga wykorzystywania całego instrumentarium środków przewidzianych przez rodo. Ważne jest to, że ustawodawca unijny promuje wykorzystywanie narzędzi zmniejszających ryzyko, niejednokrotnie zwalniając administratorów danych w takich sytuacjach z innych obowiązków.

Można powiedzieć, że przyjęty model regulacji w większym stopniu niż obecnie powoduje konieczność proaktywnego podejścia administratorów danych oraz podmiotów przetwarzających, w tym co do uwzględniania zmieniających się zagrożeń i możliwych sposobów ich minimalizacji. Niewątpliwie kluczową rolę w tym modelu będzie odgrywał inspektor ochrony danych.

Zasada rozliczalności

Pojęcie rozliczalności (*accountability*) wywodzi się z kręgu kultury anglosaskiej i jest stosowane w różnych dziedzinach, w tym przede wszystkim w: politologii, socjologii, zarządzaniu i prawie. W każdej z tych dyscyplin naukowych może być ono rozumiane odmiennie. Podobnie różne znaczenia nadaje się pojęciu rozliczalności na gruncie obecnie obowiązujących regulacji o ochronie danych osobowych. Niemniej punktem wyjścia powinna być definicja zaproponowana przez Grupę Roboczą Art. 29 w opinii nr 3/2010 w sprawie zasady rozliczalności, zgodnie z którą rozliczalność oznacza:

- wdrożenie środków (w tym wewnętrznych procedur) gwarantujących przestrzeganie przepisów o ochronie danych w związku z operacjami ich przetwarzania oraz
- sporządzenie dokumentacji wskazującej osobom, których dane dotyczą, oraz organom nadzorczym, jakie środki podjęto, aby zapewnić przestrzeganie przepisów o ochronie danych osobowych.

Wraz ze zwiększaniem się wolumenów przetwarzanych danych oraz konieczności zapewnienia odpowiednich gwarancji ochrony danych osobowych w kontekście transgranicznego przetwarzania danych osobowych, a co za tym idzie – pytaniem o warunki zapewnienia skuteczności modelu regulacji ochrony danych osobowych, zasada

rozliczalności nabiera coraz większego znaczenia, gdyż konieczne jest większe skoncentrowanie się na przeniesieniu ogólnych zasad ochrony danych na poziom praktycznych rozwiązań i procedur stosowanych w jednostkach przetwarzających dane osobowe. W optymalnej sytuacji wdrożenie zasady rozliczalności powinno prowadzić do stworzenia kompleksowych systemów zarządzania ochroną danych osobowych. Znalazło to odzwierciedlenie w pracach nad nowymi ramami ochrony danych osobowych w UE, w których zasadzie rozliczalności przypisano istotną rolę, rezygnując jednocześnie z obowiązków rejestracyjnych i notyfikacyjnych. W konsekwencji rodo przenosi punkt ciężkości z obecnie funkcjonującego modelu (zakłada on uprzednią notyfikację lub rejestrację operacji przetwarzania danych) na model, w którym to administrator danych musi zapewnić przestrzeganie przepisów o ochronie danych poprzez wdrożenie odpowiednich procedur wewnętrznych. Zgodnie z zasadą rozliczalności określoną w art. 5 ust. 2 rodo, administrator danych jest odpowiedzialny za przestrzeganie przepisów o ochronie danych i ma wykazać, że właściwie spełnił wymogi określone tymi przepisami. Innymi słowy, administrator ma być w stanie rozliczyć się z przestrzegania obowiązujących przepisów prawa przed organami ochrony danych, osobami, których dane dotyczą, oraz innymi interesariuszami.

Ocena skutków w zakresie ochrony danych oraz konsultowanie przetwarzania danych z GIODO

Rodo wprowadza dwie powiązane ze sobą instytucje: ocenę skutków dla ochrony danych osobowych oraz uprzednie konsultacje z organem nadzorczym. Zgodnie z art. 35 ust. 1 rodo:

> Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarza-

nia dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe, w szczególności w przypadku „systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną". Ocena taka jest konieczna również wtedy, gdy przetwarzane mają być na dużą skalę szczególne kategorie danych osobowych lub dane dotyczące wyroków skazujących i naruszeń prawa. Ponadto przeprowadzenia oceny wymaga systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie (art. 35 ust. 3 rodo). Niewątpliwie użyte przez ustawodawcę kryterium decydujące o konieczności przeprowadzenia oceny skutków dla ochrony danych w praktyce może wywoływać wątpliwości. Dlatego organy nadzorcze mają tworzyć i podawać do publicznej wiadomości wykazy rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych, jak również wykazy operacji, które takiemu obowiązkowi nie podlegają.

Obowiązek przeprowadzenia takiej oceny nie powinien być traktowany jako jednorazowa czynność, lecz raczej jako szerszy proces wymagający podejmowania w razie konieczności dalszych czynności, gdy zmieniają się ryzyka związane z operacjami przetwarzania danych osobowych. Jednocześnie art. 35 ust. 7 rodo określa jej elementy. Są to:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym (gdy ma to zastosowanie) prawnie uzasadnionych interesów realizowanych przez administratora;
- ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą;

– planowane środki mające na celu zaradzenie ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Rodo przewiduje również możliwość zasięgania w sprawie zamierzonego przetwarzania opinii osób, których dane dotyczą, lub ich przedstawicieli. Takie konsultacje są jednym z elementów realizacji rozliczalności administratora wobec osób, których dane dotyczą, i mogą przybrać różną formę w zależności od specyfiki operacji przetwarzania danych i kategorii osób, których dane dotyczą. Ustawodawca wprowadził pewne ograniczenia takiej możliwości ze względu na konieczność ochrony uzasadnionych interesów administratora danych. Rodo nakłada obowiązek przeprowadzenia oceny skutków dla ochrony danych na administratora danych, a nie na wyznaczonego przez niego inspektora ochrony danych, z którym jedynie się konsultuje.

Konsekwencją przeprowadzenia oceny skutków dla ochrony danych może być konieczność skonsultowania się administratora z organem nadzorczym w ramach procedury uprzednich konsultacji uregulowanych w art. 36 rodo. Zgodnie z tym przepisem, powinno to nastąpić, gdy ocena skutków dla ochrony danych wskaże, że „przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka". W świetle art. 36 ust. 2 rodo, jeżeli organ nadzorczy jest zdania, że zgłoszone mu planowane operacje przetwarzania danych osobowych stanowiłyby naruszenie postanowień ogólnego rozporządzenia (co może polegać na niedostatecznym zidentyfikowaniu lub zminimalizowaniu ryzyka przez administratora danych), to w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje udziela pisemnego zalecenia temu administratorowi, a gdy ma to zastosowanie – także podmiotowi przetwarzającemu. Jednocześnie organ nadzorczy może skorzystać z kompetencji naprawczych określonych w art. 58 rodo. Okres ten może być przedłużony o kolejne sześć

tygodni ze względu na złożony charakter zamierzonego przetwarzania. Bieg tych terminów można zawiesić do czasu, aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji.

Uwzględnienie ochrony danych osobowych w fazie projektowania oraz domyślna ochrona danych

Artykuł 25 rodo wprowadza dwie koncepcje: uwzględnianie ochrony danych w fazie projektowania oraz domyślną ochronę danych. Ustawodawca europejski, nadając charakter prawny rozwijanej już wcześniej koncepcji zapewnienia prywatności na etapie projektowania (*privacy by design*), nazwał ją zasadą uwzględnienia ochrony danych w fazie projektowania. Koncepcja ta zakłada, że wymogi dotyczące ochrony danych osobowych i prywatności powinny być uwzględniane już na wstępnych etapach projektowania usług, produktów bądź systemów mających służyć do przetwarzania danych osobowych. Takie podejście umożliwia swoiste „zaszycie" we wprowadzanych rozwiązaniach technologicznych wymogów dotyczących ochrony danych. Tym samym już na etapie projektowania kwestie ochrony danych stają się jednym z elementów, które powinny być uwzględnione w tym procesie, co daje możliwość wypracowania rozwiązań umożliwiających równoczesne zachowanie pożądanych funkcji i wymogów ochrony danych osobowych. W procesie wprowadzania produktu, usługi lub systemu informatycznego późniejsze wdrażanie mechanizmów gwarantujących ochronę danych osobowych jest dużo trudniejsze i z pewnością kosztowniejsze.

Zasada zapewnienia prywatności na etapie projektowania znalazła odzwierciedlenie w rezolucji przyjętej w 2010 r. w czasie 32. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w Jerozolimie. Podkreślono w niej, że zapewnienie prywatności na etapie projektowania jest koncepcją o charakterze holistycznym, tzn. ma zastosowanie do działalności całej organizacji oraz obejmuje: technologie informacyjne, procesy biznesowe i infrastrukturę sieciową. Rezolucja wymieniła również podstawowe zasady koncepcji zapewnienia prywatności na etapie projektowania. Są to:

- podejście proaktywne, niereaktywne i zaradcze, nienaprawcze,
- prywatność jako ustawienie domyślne,
- prywatność włączona w projekt,
- pełna funkcjonalność: suma dodatnia, a nie suma zerowa,
- ochrona od początku do końca cyklu życia informacji,
- widoczność i przejrzystość,
- poszanowanie dla prywatności użytkowników.

Uwzględnianie ochrony danych osobowych w fazie projektowania w świetle art. 25 ust. 1 rodo oznacza, że administrator zarówno na etapie planowania sposobów przetwarzania, jak i w czasie samego przetwarzania wdraża odpowiednie środki techniczne i organizacyjne, mające na celu skuteczną realizację zasad ochrony danych oraz spełnienie wymogów rodo, a także ochronę praw osób, których dane dotyczą. Wdrożenie takich rozwiązań powinno – w świetle wspomnianego artykułu – uwzględniać „(…) stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania". Ustawodawca jako przykład możliwego do wdrożenia środka podaje pseudonimizację. Jednocześnie odnotowuje fakt, że bardzo często wdrożenie zasady uwzględnienia ochrony danych osobowych w fazie projektowania będzie dotyczyło zasady minimalizacji.

Druga z omawianych koncepcji, czyli koncepcja domyślnej ochrony danych, pierwotnie dotyczyła sytuacji przystąpienia przez osobę, której dane dotyczą, do usługi świadczonej drogą elektroniczną (przede wszystkim chodziło o portale społecznościowe). Miała ona uchronić takich użytkowników przed nieświadomym udostępnianiem swoich danych w ramach takich usług szerokim kręgom odbiorców poprzez wymóg, aby domyślne ustawienia prywatności w momencie przystępowania do usługi zapewniały najwyższy poziom ochrony danych, a jego obniżenie wymagało działania użytkownika. W praktyce bowiem często się okazywało, że użytkownicy np. portali społecznościowych

nie byli świadomi zastosowanych domyślnie przez usługodawcę ustawień prywatności, a te np. umożliwiały dostęp szerokiemu kręgowi podmiotów do danych takich użytkowników. Wydaje się, że rodo rozszerzyło tę koncepcję. Zgodnie z art. 25 ust. 2 rodo, „administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych".

Certyfikacja oraz wdrażanie kodeksów postępowania

Celem kodeksów postępowania – które zgodnie z art. 40 ust. 1 rodo mają być promowane przez państwa członkowskie, organy nadzorcze, Europejską Radę Ochrony Danych oraz Komisję – jest pomoc we właściwym stosowaniu przepisów rodo. Takie kodeksy mogą bowiem doprecyzować wymogi z uwzględnieniem specyfiki różnych sektorów, w których dochodzi do przetwarzania danych osobowych. Kodeksy postępowania mogą być przyjmowane przez zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające.

Zgodnie z art. 40 ust. 2 rodo, kodeksy postępowania mogą być przyjmowane po to, aby doprecyzować zastosowanie przepisów rodo, w szczególności w odniesieniu do:

a) rzetelnego i przejrzystego przetwarzania;
b) prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach;
c) zbierania danych osobowych;
d) pseudonimizacji danych osobowych;
e) informowania opinii publicznej i osób, których dane dotyczą;
f) wykonywania przez osoby, których dane dotyczą, przysługujących im praw;

g) informowania i ochrony dzieci oraz sposobu pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem;
h) środków i procedur, o których mowa w art. 24 i 25, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32;
i) zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą;
j) przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych lub
k) postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą, w zakresie przetwarzania, bez uszczerbku dla praw osób, których dane dotyczą, na mocy art. 77 i 79.

W tym zakresie rodo wprowadza model koregulacji, gdyż kodeksy postępowań w dziedzinie ochrony danych osobowych wymagają zatwierdzenia przez organy nadzorcze. Zgodnie z art. 40 ust. 5 rodo zrzeszenia i inne podmioty chcące opracować kodeks postępowania lub zmienić bądź rozszerzyć zakres kodeksu już obowiązującego przedkładają projekt kodeksu, zmiany lub rozszerzenia właściwemu organowi nadzorczemu, który wydaje opinię o jego zgodności z przepisami ogólnego rozporządzenia i zatwierdza go, jeżeli uzna, że proponowane rozwiązania stanowią odpowiednie zabezpieczenia. Zatwierdzony kodeks jest rejestrowany i publikowany przez organ nadzorczy.

Kodeksy postępowań powinny także umożliwiać monitorowanie przestrzegania ich postanowień przez specjalne podmioty akredytowane w tym celu przez organy nadzorcze na mocy art. 42 rodo. Oprócz kodeksów postępowań rodo wprowadza mechanizmy certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych, mających świadczyć o zgodności operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające z przepisami rodo. Stosownie do art. 42 rodo certyfikacja ma być dobrowolna, a proces jej uzyskania musi być przejrzysty. Jednocześnie – tak jak w przypadku kodeksów postępowania – certyfikacja nie zwalnia administratorów danych

i podmiotów przetwarzających ze swoich obowiązków przewidzianych przepisami o ochronie danych osobowych, jak również nie wpływa na kompetencje organów nadzorczych.

Certyfikacja może być wykonywana przez podmioty certyfikacyjne lub organy nadzorcze na podstawie kryteriów określonych przez te organy lub Europejską Radę Ochrony Danych. Certyfikacji administratora lub podmiotu przetwarzającego udziela się na maksymalny okres trzech lat z możliwością jej przedłużenia po spełnieniu wymaganych warunków. Podkreślenia wymaga, że podmioty certyfikacyjne będą mogły prowadzić swoją działalność jedynie po spełnieniu określonych warunków i akredytacji, która może być cofnięta.

Odpowiedzialność za naruszenie zasad ochrony danych osobowych

Rodo wprowadza kompleksowe regulacje dotyczące sankcji, mających zastosowanie w sytuacji naruszenia przepisów o ochronie danych osobowych. Oprócz sankcji administracyjnych, nakładanych przez organy nadzorcze w ramach ich kompetencji naprawczych na mocy art. 58 ust. 2 rodo, ustawodawca przewidział możliwość nakładania administracyjnych kar pieniężnych oraz określił w pewnym zakresie zasady odpowiedzialności cywilnoprawnej.

Ustawodawca europejski, ustanawiając administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych, zdecydował się na ujednolicenie zasad ich nakładania przez organy nadzorcze. Ma to służyć wzmocnieniu i zharmonizowaniu sankcji administracyjnych oraz jest naturalną konsekwencją ujednolicenia wymogów dotyczących ochrony danych osobowych na poziomie UE. Jednolite reguły w tym zakresie stają się niezbędne do tego, by zapewnić jednolity poziom przestrzegania przepisów i uniknąć tzw. *forum shopping*, czyli przenoszenia działalności do państw, w których sankcje za naruszenie tych samych wymogów będą niższe.

Artykuł 83 ust. 2 rodo przewiduje, że administracyjne kary pieniężne nakłada się jednocześnie z nakazami określonymi w art. 58 ust. 2

rodo albo zamiast nich. Jednocześnie organy nadzorcze mają zapewnić, że kary te mają być „w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające" (art. 83 ust. 1 rodo). W powołanym artykule ujednolicone zostały kryteria, które organ nadzorczy musi wziąć pod uwagę, decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość.

Rodo określa górne limity administracyjnych kar pieniężnych, dzieląc je na dwie grupy ze względu na rodzaj naruszenia. W pierwszej grupie taka kara może być nałożona maksymalnie do wysokości 10 mln euro, a w przypadku przedsiębiorstwa do 2% jego całkowitego rocznego światowego obrotu. W drugiej grupie będzie to odpowiednio 20 mln euro i 4% obrotu.

Rozporządzenie ogólne nie przesądza, czy administracyjne kary pieniężne mogą być nakładane na podmioty publiczne, aczkolwiek daje taką możliwość państwom członkowskim. Zgodnie z art. 83 ust. 7 rodo: „każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim".

Artykuł 82 rodo wprowadza zasady odpowiedzialności odszkodowawczej za naruszenie jego przepisów. Odszkodowanie za szkodę majątkową lub niemajątkową spowodowaną naruszeniem rodo może być dochodzone przez każdą osobę od administratora lub podmiotu przetwarzającego. Co do zasady, to administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym przepisy rodo. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem tylko wtedy, gdy nie dopełnił obowiązków, które rodo nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom (art. 82 ust. 2 rodo).

Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności odszkodowawczej, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. Tym samym to na te podmioty przeniesiony został ciężar dowodu, a zatem osoby, których dane dotyczą, nie muszą tej winy wykazywać

(art. 82 ust. 3 rodo). W odniesieniu do szkód spowodowanych przetwarzaniem danych przez kilka podmiotów rodo wyraźnie przewiduje ich odpowiedzialność solidarną. Oznacza to, że jeżeli w tych samych operacjach przetwarzania uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator, jak i podmiot przetwarzający, to ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania (art. 82 ust. 4 rodo). Przy czym nie wyłącza to roszczeń regresowych między tymi podmiotami.

Notyfikacja naruszeń ochrony danych osobowych

Wśród nowych obowiązków administratorów danych oraz w pewnym zakresie również podmiotów przetwarzających należy wymienić obowiązek notyfikacji naruszeń ochrony danych osobowych, które zgodnie z art. 4 pkt 12 rodo zostały zdefiniowane jako naruszenia bezpieczeństwa „prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych".

W odróżnieniu od dotychczas obowiązujących przepisów rodo nie ogranicza obowiązku notyfikacji do niektórych sektorów, lecz ma powszechny zasięg i obejmuje wszystkich administratorów danych. Takie rozwiązanie było już stosowane w niektórych państwach członkowskich UE (np. w Irlandii i Niemczech). Na gruncie rodo dużo ważniejsze z perspektywy istnienia obowiązku notyfikacyjnego są charakter samego naruszenia bezpieczeństwa i jego potencjalne konsekwencje.

Naruszenia ochrony danych osobowych mają być zgłaszane przez administratorów danych organowi nadzorczemu. Niezależnie od zgłoszenia naruszenia organowi nadzorczemu administratorzy danych mogą również mieć obowiązek zawiadomienia o takim naruszeniu osób, których dane dotyczą. Natomiast jeżeli to podmiot przetwarzający stwierdzi naruszenie ochrony danych osobowych, to jest on obowiązany do niezwłocznego zgłoszenia naruszenia administratorowi danych.

Wprowadzony przez rodo obowiązek notyfikacyjny podlega jednak ograniczeniom. Naruszenia ochrony danych osobowych nie wymagają bowiem zgłoszenia organowi nadzorczemu wówczas, gdy jest mało prawdopodobne, by skutkowały one ryzykiem naruszenia praw lub wolności osób fizycznych. Natomiast obowiązek zawiadamiania osoby, której dane dotyczą, o takim naruszeniu, zgodnie z art. 34 ust. 1 rodo, pojawi się jedynie wtedy, gdy takie zdarzenie „(…) może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych". Administrator danych nie będzie miał obowiązku zawiadomienia osób, których dane dotyczą, jeżeli wdrożył odpowiednie środki ochrony o charakterze technicznym i organizacyjnym oraz zastosował je do danych osobowych, których dotyczy incydent. Ustawodawca europejski jako przykład wdrożenia takich środków podał sytuację uniemożliwienia dostępu do takich danych osobom nieupoważnionym dzięki wcześniejszemu zastosowaniu szyfrowania. Kolejną przesłanką zwolnienia z obowiązku zawiadomienia jest zastosowanie przez administratora danych środków o charakterze następczym, które eliminują prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby. Wreszcie w sytuacji, gdy zawiadomienie poszczególnych osób, których dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku, może być wystarczające wydanie publicznego komunikatu lub zastosowanie podobnego środka, dzięki któremu osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

Administrator danych jest obowiązany zgłosić naruszenie organowi nadzorczemu niezwłocznie, w miarę możliwości nie później niż w terminie 72 godzin od stwierdzenia naruszenia. Jeżeli nie wszystkie wymagane informacje dotyczące naruszenia są dostępne od razu, to rodo dopuszcza ich sukcesywne podanie. Niemniej jeżeli samo zgłoszenie nastąpi już po upływie 72 godzin, to należy dołączyć do niego wyjaśnienie przyczyny opóźnienia. Natomiast poinformowanie osób, których dane dotyczą, jeżeli zachodzi taki obowiązek, powinno nastąpić bez zbędnej zwłoki, tak aby umożliwić im podjęcie niezbędnych działań zapobiegawczych.

Nowe zadania i uprawnienia organu nadzorczego

Na przestrzeni ostatnich lat niezależne organy ochrony danych, zwane również organami nadzorczymi[1], stały się kluczowym elementem europejskiego modelu ochrony danych osobowych. Ich szczególny status, rola i zadania znalazły odzwierciedlenie w art. 28 dyrektywy 95/46/WE, co później zostało potwierdzone w art. 8 Karty Praw Podstawowych UE, w art. 16 Traktatu o Funkcjonowaniu UE, a także w orzecznictwie Trybunału Sprawiedliwości UE, który określił wysokie wymagania w odniesieniu do gwarancji niezależności organów ochrony danych osobowych. Rozwiązania przyjęte w rodo wykorzystują dotychczasowe standardy i je rozwijają. Jednym z głównych celów unijnej reformy prawa ochrony danych osobowych było bowiem wzmocnienie pozycji ustrojowej niezależnych organów ochrony danych osobowych, które dzięki temu mają efektywniej egzekwować przestrzeganie przepisów o ochronie danych osobowych na terytorium swoich krajów.

Wzmocnienie pozycji prawnej organów nadzorczych zostało zrealizowane poprzez przyznanie im nowych, szerszych kompetencji oraz zagwarantowanie im prawnych gwarancji pełnej niezależności. Przejawiają się one m.in. w nałożeniu na państwa członkowskie obowiązku zapewnienia organom ochrony danych niezbędnych środków organizacyjnych, technicznych i finansowych. Porównując ukształtowanie statusu, zadań i kompetencji organów nadzorczych w dotychczasowych przepisach dyrektywy 95/46/WE i we wdrażających ją przepisach ustaw krajowych oraz w rodo, wyraźnie widać, że intencją ustawodawcy unijnego było zlikwidowanie obecnych różnic w kompetencjach krajowych organów ochrony danych i zapewnienie ich ujednolicenia.

Z tego powodu rodo wprowadza jednolity katalog zadań oraz kompetencji organów nadzorczych, czerpiąc z dotychczasowych rozwiązań przyjętych w prawie unijnym oraz wprowadzając nowe. Wśród nowych rozwiązań, w szczególności nieznanych dotąd polskim przepisom o ochronie danych osobowych, należy wymienić kompetencję

1 W Polsce takim organem jest GIODO.

do nakładania administracyjnych kar finansowych. Jednakże równie ważne jest większe podkreślenie przez ustawodawcę europejskiego edukacyjnej i doradczej roli organów ochrony danych oraz uwzględnienie ich roli w nowych mechanizmach ustanawiania i funkcjonowania systemów certyfikacji oraz samoregulacji.

Zgodnie z art. 57 rodo, do zadań organów nadzorczych należy nie tylko monitorowanie i egzekwowanie przestrzegania przepisów o ochronie danych, rozpatrywanie skarg osób, których dane dotyczą, i prowadzenie związanych z tym postępowań, ale również upowszechnianie wiedzy w tym zakresie, w szczególności podejmowanie działań edukacyjnych skierowanych do dzieci, a także upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o spoczywających na nich obowiązkach. Organy nadzorcze mają również doradzać parlamentom narodowym, rządom oraz innym instytucjom i organom w sprawie aktów prawnych i środków administracyjnych, jak również udzielać osobom, których dane dotyczą, na ich żądanie informacji o wykonywaniu praw przysługujących im na mocy rodo. Ważnym zadaniem każdego organu nadzorczego jest współpraca z innymi organami nadzorczymi, w tym wymiana informacji oraz wzajemna pomoc oraz udział w pracach Europejskiej Rady Ochrony Danych. W praktyce organów ochrony danych osobowych coraz ważniejsze jest monitorowanie rozwoju technologii informacyjno-komunikacyjnych, nowych modeli biznesowych i zmian mających wpływ na ochronę danych osobowych w innych dziedzinach. W związku z nałożeniem na administratorów danych obowiązku przeprowadzenia oceny skutków dla ochrony danych organy nadzorcze mają również za zadanie ustanowienie i prowadzenie wykazów operacji wymagających przeprowadzenia takiej oceny i takich, które jej nie wymagają. Powiązane z tym jest udzielanie pisemnych zaleceń w ramach prowadzonych uprzednich konsultacji.

Wśród zadań organów nadzorczych należy również wymienić różne zadania dotyczące kodeksów postępowania oraz mechanizmów certyfikacji. Ponadto organy nadzorcze zatwierdzają różne instrumenty

prawne umożliwiające przekazywanie danych osobowych do państw trzecich, które nie zapewniają odpowiedniego poziomu ochrony. Niezależnie od wymienionych już zadań każdy organ ochrony danych ma prowadzić wewnętrzny rejestr naruszeń rodo i działań naprawczych podjętych zgodnie z art. 58 ust. 2 rodo. Każdy organ nadzorczy bezpłatnie wypełnia zadania na rzecz osoby, której dane dotyczą, i inspektora ochrony danych. Organ jest zobowiązany do ułatwiania wnoszenia skarg przez osoby, których dane dotyczą, w szczególności poprzez udostępnienie odpowiedniego formularza w formie elektronicznej (art. 57 ust. 2 rodo). Jednocześnie ustawodawca europejski dopuszcza pobranie opłaty w rozsądnej wysokości wynikającej z kosztów administracyjnych albo odmowę podjęcia żądanych działań, jeżeli takie żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności ze względu na swą powtarzalność (art. 57 ust. 4 rodo).

Uprawnienia organów nadzorczych

- wydawanie ostrzeżeń skierowanych do administratora lub podmiotu przetwarzającego, gdy planowane operacje przetwarzania danych mogą naruszać przepisy rodo;
- udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu, gdy operacje przetwarzania danych naruszają przepisy ogólnego rozporządzenia;
- nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądań osoby, której dane dotyczą, w zakresie realizacji jej uprawnień;
- nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania prowadzonych operacji przetwarzania danych do przepisów rodo;
- nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- wprowadzanie czasowego lub całkowitego ograniczenia, a nawet zakazu przetwarzania danych;
- nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;

- cofnięcie certyfikatu lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikatu lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
- nałożenie administracyjnej kary pieniężnej;
- wstrzymanie przekazywania danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

Oprócz kompetencji naprawczych organom nadzorczym przyznano kompetencje do wydawania zezwoleń i uprawnienia doradcze obejmujące: udzielanie porad administratorowi w ramach uprzednich konsultacji; wydawanie opinii przeznaczonych m.in. dla parlamentu narodowego, rządu państwa członkowskiego oraz ogółu społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych; wydawanie uprzednich zezwoleń na określone operacje przetwarzania danych, jeżeli taki obowiązek przewiduje prawo krajowe; opiniowanie i zatwierdzanie projektów kodeksów postępowania; akredytowanie podmiotów certyfikujących; udzielanie certyfikatów i zatwierdzanie kryteriów certyfikacji. Ponadto organy nadzorcze przyjmują standardowe klauzule ochrony danych; zezwalają na inne klauzule umowne oraz na uzgodnienia administracyjne w sprawie przekazywania danych, a także zatwierdzają wiążące reguły korporacyjne.

Ujednolicenie zadań i kompetencji organów ochrony danych osobowych będzie szczególnie istotne w odniesieniu do tzw. transgranicznego przetwarzania. Zgodnie z art. 4 pkt 23 rodo, pojęcie to oznacza „przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim". Rodo określa

jurysdykcję organu nadzorczego w sprawach transgranicznych oraz wprowadza procedury współpracy pomiędzy organami nadzorczymi, których taka sprawa może dotyczyć (w tym mechanizm kompleksowej współpracy), oraz w ostateczności w razie konfliktu wprowadza między zaangażowanymi organami możliwość wydawania wiążących decyzji przez Europejską Radę Ochrony Danych.

Piotr Drobek – zastępca dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej.

Rozdział II
Od postępowania rejestracyjnego do uprzednich konsultacji z organem nadzorczym

Model kontroli wstępnej operacji przetwarzania, który wynikał z dyrektywy 95/46/WE, i zgłaszania w tym celu zbiorów danych osobowych do rejestracji GIODO przejdzie do historii 25 maja 2018 r. Rodo wprowadza w to miejsce – jako elementy nowej procedury opartej na ocenie ryzyka planowanych operacji przetwarzania danych osobowych – nowe rozwiązania: ocenę skutków przetwarzania dla ochrony danych osobowych dokonywaną przez administratora (art. 35 rodo) oraz uprzednie konsultacje z organem nadzorczym (art. 36 rodo). W sytuacji gdy ryzyko zagrożenia bezpieczeństwa danych jest wysokie, dokonanie oceny to obowiązek administratora danych. Jeśli analiza ryzyka potwierdzi duże prawdopodobieństwo zaistnienia negatywnych skutków dla prywatności, administrator konsultuje się z organem nadzorczym, aby zminimalizować niebezpieczeństwo.

Działania organu nadzorczego i administratora danych mające na celu definiowanie i eliminowanie zagrożeń dla praw i wolności osób, których dane dotyczą, jeszcze przed rozpoczęciem przetwarzania danych, nie są nowością (np. zgłoszenie zbioru danych do rejestracji GIODO zawierające informacje dotyczące stanu faktycznego przetwarzania danych i kontrola wstępna dokonywana przez ten organ). Jednak nowe przepisy mają służyć większej ich skuteczności w świetle wyzwań stawianych np. przez rozwój nowych technologii, który daje możliwość przetwarzania danych osobowych stwarzającego zagrożenia nieznane w dobie uchwalania i implementacji do prawa polskiego dyrektywy 95/46/WE. Zmienia się podejście dotyczące sposobu działania administratora danych i organu nadzorczego przed rozpoczęciem przetwarzania danych w celu ochrony prywatności. Rodo znosi ogólny obowiązek zawiadamiania organu o przetwarzaniu danych osobowych i koncentruje się na tych operacjach przetwarzania, które,

ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw i wolności osób, których dotyczą. Ewidentnie wzrasta rola administratora danych jako aktywnego podmiotu, na którym ciąży obowiązek zdefiniowania zagrożeń i podjęcia działań w celu ich wyeliminowania.

W świetle przepisów dyrektywy 95/46/WE brak obowiązku zgłoszenia zbioru danych do rejestracji organowi nadzorczemu to wyjątek od zasady, który następuje w ściśle określonych przez ustawę przypadkach (są one wskazane w katalogu zwolnień z obowiązku rejestracji określonego w uodo). Zgodnie z rodo, organ nadzorczy ustanowi i poda do publicznej wiadomości wykaz rodzajów operacji przetwarzania, które podlegają wymogowi oceny skutków dla ochrony danych (lub wykaz operacji niepodlegających temu wymogowi). Rodo stanowi, że są to w szczególności operacje na danych z użyciem nowych technologii, polegające na systematycznej, kompleksowej ocenie czynników osobowych (np. profilowaniu), które są podstawą decyzji wywołującej skutki prawne wobec osoby fizycznej lub w podobny sposób wpływające na osobę fizyczną. Do operacji przetwarzania, które wymagają oceny ryzyka, należy także przetwarzanie na dużą skalę szczególnych kategorii danych.

Podmiotem zobowiązanym do dokonania oceny ryzyka przed rozpoczęciem przetwarzania jest administrator danych, niezależnie od tego, czy zamierza przetwarzać dane osobowe samodzielnie, czy w przetwarzaniu będzie brał udział podmiot działający w jego imieniu. Jeśli administrator uzna, że przeprowadzona ocena potwierdza wysokie ryzyko dla ochrony danych osobowych i niezbędne jest zastosowanie środków minimalizujących zagrożenie, to konsultuje się z organem nadzorczym w sposób określony w rodo.

Administrator informuje organ nadzorczy o celach i sposobach zamierzonego przetwarzania, wskazuje środki służące zabezpieczeniu danych osobowych, dane kontaktowe inspektora ochrony danych, jeśli go powołał, a także jest zobowiązany podać wszelkie inne informacje, których organ zażąda.

Najistotniejszą różnicą w stosunku do procedury zgłaszania zbiorów danych do rejestracji jest obowiązek dołączenia do wniosku o konsultacje oceny skutków przetwarzania dla prywatności osób, których dane dotyczą. Właśnie w tym zawiera się sens nowego podejścia wynikającego z rodo.

Ocena przeprowadzona przez administratora danych przed rozpoczęciem przetwarzania powinna zawierać co najmniej:

– systematyczny opis planowanych operacji i ich celów,
– ocenę, czy planowane operacje przetwarzania są niezbędne i proporcjonalne do celów,
– ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
– charakterystykę planowanych środków zaradczych, które mają zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia ogólnego.

Gdy organ nadzorczy będzie zdania, że przetwarzanie stanowiłoby naruszenie rodo, to na piśmie zaleca administratorowi określone działania i może skorzystać z uprawnień, o których mowa w art. 58 rodo, czyli np. nakazać dostosowanie operacji przetwarzania do przepisów rodo, wydać ostrzeżenie dotyczące możliwości naruszenia przepisów poprzez planowane operacje na danych, wprowadzić czasowe lub całkowite ograniczenie przetwarzania (w tym zakazać przetwarzania danych), nałożyć karę pieniężną w zależności od okoliczności sprawy.

Obecnie GIODO, jeśli naruszone są zasady przetwarzania, ma obowiązek stosowania uprawnień władczych (wydaje decyzję o odmowie rejestracji zbioru ze stosownymi nakazami), nie stosuje uprawnień doradczych, jak udzielanie porad zgodnie z procedurą uprzednich konsultacji. Z powyższego, bardzo syntetycznego porównania obowiązku zgłaszania do rejestracji GIODO zbiorów danych oraz procedury oceny ryzyka i konsultacji z organem nadzorczym przed rozpoczęciem przetwarzania danych można wywnioskować, że określony w rodo sposób konsultacji z organem przed rozpoczęciem przetwarzania danych w przypadku szczególnie niebezpiecznych operacji przetwarzania

zawiera pewne formalne podobieństwa do obowiązku zgłoszenia zbioru do rejestracji organowi nadzorczemu i kontroli wstępnej dokonywanej przez organ, wynikającej z obecnej uodo. Jednak podejście do kwestii bezpieczeństwa danych zmienia się w istotny sposób. W rodo przyjęto bowiem zasadę *risk based approach* opartą na analizie ryzyka. Rodo kładzie szczególny nacisk na samokontrolę administratora danych i realizację zasady uwzględniania ochrony danych w fazie projektowania (*privacy by design*). Administrator danych będzie zobowiązany ocenić, czy i w jaki sposób planowany rodzaj przetwarzania danych wpłynie na prywatność osób, których dane dotyczą, oraz czy zagrożenie jest duże. Będzie także zobowiązany zastosować konkretne rozwiązania, które w jego ocenie wyłączą lub zminimalizują ryzyko. Organ nadzoru zweryfikuje skuteczność działań administratora i wyda w razie potrzeby pisemne zalecenia; może też zastosować bardziej dolegliwe środki. Procedura uprzednich konsultacji i poprzedzającej ją oceny ryzyka jest dedykowana szczególnie skomplikowanym i zagrażającym prywatności operacjom przetwarzania danych, odbywającym się z użyciem innowacyjnych technologii, i zastępuje ogólny obowiązek rejestracyjny.

Nowością jest czynny udział w tych działaniach inspektora ochrony danych, dlatego tak istotna jest jego wiedza również z zakresu merytorycznego działania administratora. Inspektor ochrony danych ma za zadanie doradzić administratorowi, które planowane operacje powinny być poddane kontroli, jaką przyjąć metodologię, czy zlecić wykonanie oceny podmiotowi zewnętrznemu, czy też wykonać ją własnymi siłami. Inspektor powinien sprawdzić, czy ocena skutków przetwarzania została przeprowadzona prawidłowo i czy uzyskane wnioski są zgodne z założeniami rodo. Należy podkreślić jednak, że inspektor ochrony danych nie przeprowadza oceny ryzyka – odpowiedzialność w tym zakresie ponosi administrator danych osobowych.

Dorota Krajewska-Kekusz – dyrektor Departamentu Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych.

Rozdział III
Zmiana statusu i zadań ABI po wejściu do stosowania rodo

Rodo stanowiące obok tzw. dyrektywy policyjnej „nowe ramy ochrony danych osobowych" wprowadza wiele, od dawna potrzebnych zmian i nowych rozwiązań w sektorze ochrony danych osobowych. Mają one na celu nie tylko zapewnienie jednolitego i spójnego systemu ochrony danych osobowych na terenie Unii Europejskiej, lecz także unowocześnienie i podniesienie jego efektywności. Wdrożenie nowych przepisów będzie wymagało od podmiotów odpowiedzialnych za przetwarzanie danych proaktywnego podejścia do stosowania nowych przepisów i wybierania rozwiązań dostosowanych do konkretnej struktury organizacyjnej i rodzaju działalności administratorów danych i podmiotów przetwarzających oraz do charakteru, zakresu, kontekstu i celów prowadzonego przez nich przetwarzania danych osobowych. Przestrzeganie nowych przepisów będzie wymagać identyfikowania ryzyka związanego z przetwarzaniem, jego oceny pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz wprowadzania skutecznych praktyk pozwalających zminimalizować to ryzyko. Poprzez wprowadzenie w przepisach rodo zasady rozliczalności administratorzy danych i podmioty przetwarzające dane zostali zobowiązani do stałej gotowości wykazania wewnętrznego przestrzegania rodo, a zatem poprawności i skuteczności zastosowanych rozwiązań.

Temu nowemu podejściu do ochrony danych osobowych i licznym wyzwaniom z nim związanym trudno będzie sprostać bez kompetentnego, fachowego wsparcia, jakim niewątpliwie będą inspektorzy ochrony danych osobowych (obecni ABI). Często podkreśla się, że dysponujący odpowiednią wiedzą i umiejętnościami inspektorzy mają odegrać kluczową rolę w zapewnieniu zgodności przetwarzania danych osobowych z nowymi unijnymi regulacjami prawnymi i stanowić fundament nowego, skutecznego systemu ochrony danych.

Obowiązek wyznaczania inspektora ochrony danych

Prawodawca unijny w rodo wprowadził w określonych przypadkach obligatoryjne wyznaczenie inspektorów ochrony danych, wzmocnił ich niezależność i pozycję, doprecyzował wymogi dotyczące ich fachowego przygotowania (wiedzy i umiejętności) oraz wprowadził ochronę tych osób przed negatywnymi skutkami działań podejmowanych na rzecz ochrony danych osobowych. Określił również zakres zadań inspektorów w sposób, który wskazuje, że osoba ta ma przede wszystkim pełnić rolę doradczą i weryfikacyjną wobec działań i decyzji administratorów danych i podmiotów przetwarzających dane.

Wprowadzenie obowiązku wyznaczenia inspektora ochrony danych dla określonych kategorii administratorów danych i – co ważne – dla podmiotów przetwarzających niewątpliwie podnosi status i znaczenie inspektorów ochrony danych. Obowiązek ich wyznaczenia będą mieli administratorzy danych i podmioty przetwarzające będące organami lub podmiotami publicznymi (z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości). Ponadto obowiązek taki będzie dotyczył administratorów i procesorów, których główna działalność polega na operacjach przetwarzania danych wymagających – ze względu na swój charakter, zakres lub cele – regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę oraz administratorów i procesorów, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Powyższy obowiązek został określony w art. 37 ust. 1 rodo. Przepis ten posługuje się kilkoma kryteriami, wymagającymi wykładni ze względu na ich treść (chodzi o sformułowania: „główna działalność", „regularne i systematyczne monitorowanie" i „na dużą skalę"). W jej dokonywaniu pomocne mogą być bezpośrednie lub pośrednie wskazówki interpretacyjne zawarte w motywach rodo stanowiących jego kontekst normatywny, np.: „W sektorze prywatnym przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności" (motyw 97 rodo)

lub ocena skutków dla ochrony danych powinna „mieć zastosowanie w szczególności do operacji przetwarzania o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą" (motyw 91 rodo). Ocena kryterium „dużej skali" z pewnością będzie musiała być dokonywana w kontekście konkretnego stanu faktycznego, niemniej z przytoczonych fragmentów rodo wynika, że w poszczególnych przypadkach konieczne może być uwzględnienie proporcji, np. wielkości terytorium, na którym następować będzie przetwarzanie danych osobowych (im większe terytorium, tym większa liczba danych będzie podstawą uznania, że przetwarzanie odbywa się na dużą skalę). Do maja 2018 r. istotny wpływ na doprecyzowanie art. 37 będzie mieć również Grupa Robocza Art. 29, a po tej dacie – Europejska Rada Ochrony Danych. Oprócz art. 37 ust. 1 rodo obowiązek wyznaczenia inspektora ochrony danych osobowych może wprowadzić prawo Unii Europejskiej lub państwo członkowskie w prawie krajowym. W pozostałych przypadkach wyznaczenie inspektora ochrony danych będzie dobrowolne.

Istotną nowością w zakresie zasad wyznaczania inspektorów ochrony danych jest określenie warunków wyznaczenia jednego inspektora ochrony danych dla kilku administratorów danych lub podmiotów przetwarzających będących podmiotami publicznymi lub w ramach grupy przedsiębiorstw. Ponadto art. 37 ust. 6 rodo wyraźnie przesądza, że inspektor ochrony danych może być zarówno członkiem personelu administratora danych lub podmiotu przetwarzającego, jak i wykonywać swoją funkcję na podstawie umowy o świadczenie usług. Obecnie na gruncie polskim funkcję ABI wykonują zarówno osoby będące pracownikami administratorów danych, jak i osoby, które zawarły z administratorem danych umowę cywilnoprawną. Uodo nie zawiera przepisu wprost odnoszącego się do tego zagadnienia. Niewątpliwie rodzaj stosunku prawnego łączącego administratora danych i ABI ma bezpośredni wpływ na przesłanki i zasady ponoszenia odpowiedzialności za prawidłowe

wykonywanie obowiązków przypisanych administratorowi bezpieczeństwa informacji. Model odpowiedzialności pracowniczej różni się bowiem od reżimu odpowiedzialności kontraktowej. W przypadku umowy cywilnoprawnej wiele w tym zakresie zależeć może od treści umowy i jej postanowień w zakresie zasad i sposobu egzekwowania odpowiedzialności za niewykonanie lub nienależyte wykonanie wynikających z niej zobowiązań.

Kwalifikacje do pełnienia funkcji

Wybór odpowiedniej osoby do pełnienia funkcji inspektora ochrony danych to ważna decyzja wymagająca odpowiedzialności i rzetelnego rozeznania. Jednym z podstawowych kryteriów wyboru powinno być należyte merytoryczne przygotowanie do pełnienia tej funkcji. Posiadanie przez ABI odpowiedniej wiedzy w dziedzinie ochrony danych osobowych jest bowiem niezbędnym warunkiem umożliwiającym wykonywanie funkcji ABI. W rodo wymóg odpowiedniego fachowego przygotowania inspektora ochrony danych został istotnie wyeksponowany i doprecyzowany. **Inspektor ochrony danych osobowych ma być wyznaczany na podstawie kwalifikacji zawodowych – a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych osobowych.** Poziom wiedzy inspektora ma być ustalany w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający (motyw 97 rodo), a zatem w kontekście specyfiki i konkretnych potrzeb administratora danych i podmiotu przetwarzającego dane. Znaczenie fachowej wiedzy dla prawidłowego wykonywania tej funkcji podkreślone zostało ponadto przez zobowiązanie administratorów danych i procesorów do zapewnienia inspektorowi ochrony danych zasobów niezbędnych do utrzymania jego wiedzy fachowej. Obowiązek uaktualniania wiedzy i zapewnienia na to środków finansowych jest w pełni uzasadniony – szczególnie w świetle wyzwań związanych z szybkim rozwojem technologii informacyjno-komunikacyjnych oraz wielkoskalowych metod przetwarzania i wymiany danych.

Ponadto rodo wprost zobowiązuje administratorów danych oraz podmioty przetwarzające do zapewnienia inspektorowi ochrony danych dostępu do danych osobowych i operacji przetwarzania oraz do niezwłocznego i właściwego włączania go we wszystkie sprawy dotyczące ochrony danych osobowych. Dokładne informacje na temat wszystkich procesów przetwarzania danych, wszystkich planowanych i realizowanych przedsięwzięć, usług i systemów związanych z przetwarzaniem danych osobowych mają być zatem nieodzownym składnikiem wiedzy inspektora ochrony danych. Dzięki temu rozwiązaniu inspektor ma zawsze dysponować kompletnymi informacjami umożliwiającymi pełną i rzetelną ocenę działalności administratora i podmiotu przetwarzającego w zakresie przestrzegania rodo. Niewątpliwie wiedza inspektora ochrony danych powinna obejmować też dobrą znajomość profilu działalności administratora danych osobowych i podmiotu przetwarzającego, związanych z tym profilem wymogów prawnych oraz szczegółów funkcjonowania danej organizacji.

Niezależność inspektora ochrony danych

Obok fachowej wiedzy kolejnym bardzo istotnym warunkiem, jaki musi być spełniony w odniesieniu do inspektora ochrony danych, jest wykonywanie jego funkcji w sposób niezależny. Motyw 97 rodo wskazuje, że inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora, czy też wykonują swoje usługi na podstawie umowy o świadczenie usług – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny. Pojęcie niezależności należy odnosić przede wszystkim do wykonywania przez inspektora jego obowiązków i zadań, a zatem odczytywać je w sensie merytorycznym. Jeśli zasadniczymi zadaniami inspektora są doradzanie w zakresie przestrzegania rodo oraz monitorowanie jego przestrzegania, to zadania te mogą być realizowane jedynie przy założeniu, że swoje oceny i zalecenia inspektor może formułować w sposób suwerenny, wolny od jakichkolwiek nacisków i wpływów. W art. 38 ust. 3 rodo wprowadzony został obowiązek zapewnienia przez administratorów danych i podmioty przetwarzające,

aby inspektor ochrony danych nie otrzymywał instrukcji co do wykonywania zadań. Ponadto wykonywanie innych obowiązków, niezwiązanych z ochroną danych, dopuszczalne jest jedynie wtedy, gdy obowiązki takie nie będą powodowały konfliktu interesów (art. 38 ust. 6 rodo). Oznacza to, że obowiązki inspektorów ochrony danych powinny być traktowane priorytetowo, inne zaś zadania mogą być realizowane tylko wówczas, gdy nie będzie to przeciwstawne skutecznemu zapewnianiu ochrony danych osobowych i będzie możliwe pod względem czasowym i organizacyjnym. Również obecnie, na gruncie uodo, powierzenie ABI innych zadań możliwe jest jedynie wówczas, gdy nie naruszy to prawidłowego wykonania zadań ABI.

Inspektor ochrony danych ma podlegać najwyższemu kierownictwu administratora lub podmiotu przetwarzającego, a zatem nie są dopuszczalne sytuacje, w których inspektor podlega jakimkolwiek innym osobom lub podmiotom. Podległość najwyższemu kierownictwu jest jedną z gwarancji niezależnej, wysokiej pozycji inspektora ochrony danych w strukturze administratora danych, a ponadto skraca drogę raportowania, co ma istotne znaczenie w razie konieczności podejmowania szybkich działań naprawczych w sytuacji naruszenia ochrony danych osobowych.

Do ważnych, nowych rozwiązań w zakresie gwarancji niezależności inspektora należy nałożony wprost na administratorów danych i podmioty przetwarzające obowiązek wspierania inspektora ochrony danych w wypełnianiu przez niego zadań, m.in. przez wspomniane już wyżej zapewnienie inspektorowi dostępu do danych osobowych i operacji przetwarzania oraz wiedzy o każdej sprawie dotyczącej ochrony danych osobowych. Ten obowiązek ma zapobiegać próbom ograniczania inspektorowi ochrony danych dostępu do niezbędnych dla realizacji jego zadań informacji. Realizując ten obowiązek, administratorzy danych i podmioty przetwarzające (zwłaszcza ci, którzy są organizacjami o dużej, złożonej strukturze) powinni wprowadzić wewnętrzne zasady i procedury, które zapewnią w tym zakresie wydajny i szybki przepływ informacji dotyczących ochrony danych.

Wspieranie inspektora w wykonywaniu jego funkcji ma polegać również na zapewnieniu mu zasobów niezbędnych do wykonania jego obowiązków. Od początku 2015 r. rozwiązanie takie przewiduje również uodo, zgodnie z którą funkcję ABI może pełnić osoba mająca zapewnione środki i organizacyjną odrębność, niezbędne do niezależnego wykonywania przez niego zadań, przy czym określenie „środki" należy rozumieć szeroko – w sensie zarówno organizacyjnym, jak i finansowym. Niewątpliwie wymóg ten ma największe znaczenie dla ABI będących pracownikami administratorów danych, ponieważ ABI działający na podstawie umowy cywilnoprawnej przeważnie posiadają organizacyjną odrębność, a środki niezbędne do wykonywania zadań zostają zabezpieczone w ramach umowy zawartej z administratorem danych.

Inspektor ochrony danych zobowiązany został również do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego, co jest uzasadnione zarówno względami bezpieczeństwa danych osobowych, jak i wolą wzmocnienia zaufania do inspektorów ze strony administratorów danych i podmiotów przetwarzających. Na gruncie uodo obowiązek zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia adresowany jest do wszystkich osób upoważnionych do przetwarzania danych (mówi o tym art. 39 ust. 2 uodo).

Jedną z ważnych i nowych gwarancji niezależności inspektora ochrony danych jest przepis, zgodnie z którym inspektor nie może być ukarany lub odwołany za wypełnianie swoich zadań (art. 38 ust. 3 rodo). Jest to jedyny przepis w rodo dotyczący zagadnienia odwołania inspektora ochrony danych. Warto jednak zauważyć, że stosownie do art. 83 ust. 4 pkt a rodo, naruszenia wszystkich przepisów bezpośrednio odnoszących się do inspektorów ochrony danych osobowych (art. 37–39 rodo) podlegają administracyjnej karze pieniężnej do 10 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Administracyjne kary pieniężne grożą zatem zarówno w przypadku niewłaściwej realizacji przez administratorów danych i podmioty przetwarzające obowiązku

wyznaczania inspektora ochrony danych i zapewnienia mu określonych warunków wykonywania funkcji, jak i w przypadku nienależytego wykonywania zadań przez inspektorów ochrony danych.

Zadania inspektora ochrony danych

W zakresie zadań inspektora ochrony danych osobowych art. 39 rodo wymienia na pierwszym miejscu wskazane już wyżej informowanie i doradzanie w zakresie obowiązków ciążących na administratorze, podmiocie przetwarzającym i pracownikach oraz monitorowanie przestrzegania przepisów i polityk w dziedzinie ochrony danych osobowych. Taki sposób określenia zadań inspektora ochrony danych osobowych powoduje, że zadania te są ściśle powiązane z obowiązkami administratorów danych, podmiotów przetwarzających oraz ich pracowników. Rodo przewiduje wiele nowych obowiązków i zadań administratorów danych i podmiotów przetwarzających, z których wiele związanych jest przede wszystkim ze wzmocnieniem praw podmiotów danych. Tytułem przykładu wskazać można, że nowe unijne przepisy rozbudowują obowiązki informacyjne wobec osób, których dane dotyczą, przyznają podmiotom danym nowe uprawnienia, takie jak „prawo do bycia zapomnianym" i „prawo do przenoszenia danych". Wprowadzony zostaje również obowiązek zgłaszania podmiotom danych i organowi nadzorczemu naruszeń ochrony danych osobowych. Niewątpliwie istotnym polem dla działań doradczych i weryfikacyjnych inspektorów ochrony danych będzie stosowanie przez administratorów danych i podmioty przetwarzające takich mechanizmów, jak: ocena skutków dla ochrony danych (*privacy impact assessment*) oraz uwzględnianie prywatności w fazie projektowania i w ustawieniach domyślnych (*privacy by design* oraz *privacy by default*). Administratorzy danych i podmioty przetwarzające, którzy wyznaczą inspektorów ochrony danych, będą korzystać z zaleceń i konsultacji co do oceny skutków dla ochrony danych. Ponadto będą mogli liczyć na monitorowanie wykonania przeprowadzonej oceny, ponieważ takie zadania zostały wprost nałożone na inspektorów ochrony danych w art. 39 ust. 1 pkt c rodo.

Zadania realizowane przez inspektora ochrony danych mają być jednym z ważniejszych elementów nowego systemu ochrony danych osobowych. W systemie tym przestrzeganie przepisów o ochronie danych monitorować mają zarówno sami administratorzy danych i podmioty przetwarzające dane wspomagani przez wyznaczonych inspektorów ochrony danych (motyw 97 rodo), jak i organy nadzorcze, których zasadniczym zadaniem jest monitorowanie i egzekwowanie rodo (art. 57 ust. 1 pkt a rodo). W celu skonsolidowania tego systemu i zapewnienia jego efektywności w katalogu zadań inspektorów ochrony danych wyraźnie zapisano obowiązek współpracy z organem nadzorczym. Inspektor ochrony danych osobowych zobowiązany będzie pełnić funkcję punktu kontaktowego dla organu nadzorczego w zakresie uprzednich konsultacji, o których mowa w art. 36 rodo, ale też we wszelkich innych sprawach.

Do zadań inspektora należeć będzie również obowiązek pełnienia funkcji punktu kontaktowego dla osób, których dane dotyczą, mimo że obowiązek taki nie został umieszczony w katalogu zadań określonych w art. 39 rodo. Na mocy art. 38 ust. 4 rodo osoby, których dane dotyczą, uprawnione zostały bowiem wprost do kontaktowania się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rodo. Poprzez wprowadzenie takiego rozwiązania inspektorzy ochrony danych będą musieli udzielać pomocy i wyjaśnień dotyczących przetwarzania danych osobowych konkretnych osób oraz przysługujących tym osobom uprawnień w każdym przypadku, gdy osoby te zwrócą się do nich z takim wnioskiem. Można przewidywać, że obowiązek ten może okazać się w praktyce zadaniem wymagającym tak dużych nakładów czasu i pracy, że w niektórych instytucjach uzasadnione będzie powołanie do jego realizacji nawet zespołu przygotowanych merytorycznie osób.

Wszystkie zadania inspektora ochrony danych mają być wypełniane z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, a także charakteru, zakresu, kontekstu i celów przetwarzania

danych. Konieczne zatem będzie podejście indywidualne i elastyczne umożliwiające adaptację rozwiązań do konkretnych potrzeb i zagrożeń związanych z procesami przetwarzania danych. Wymóg ten oznacza również, że w przypadku większych, bardziej skomplikowanych lub obciążonych większym ryzykiem operacji przetwarzania danych wprowadzone środki powinny być bardziej zaawansowane. Skuteczność zastosowanych środków powinna być regularnie sprawdzana.

Cenne dotychczasowe doświadczenia

Obecny sposób uregulowania statusu i funkcji ABI w polskiej uodo w dużej mierze odpowiada rozwiązaniom przyjętym w rodo. Jest tak dlatego, że w czasie, gdy tworzono nowe przepisy uodo znany był już projekt rodo.

Uodo zobowiązuje administratorów danych do zapewnienia ABI niezależnego sprawowania funkcji, a jednym z jego głównych zadań czyni zapewnienie przestrzegania przepisów o ochronie danych osobowych. Wprawdzie sposób wyznaczenia zadań ABI w dalszym ciągu bardziej opiera się na szczegółowych przepisach prawa (zawartych w rozporządzeniach wykonawczych do uodo) niż na ogólnej dyspozycji „należytego uwzględnienia ryzyka" (art. 39 ust. 2 rodo), ale można w tym widzieć określone korzyści dla zdobywania fachowej wiedzy i doświadczenia przez ABI oraz kształtowania bardziej wydajnego systemu ochrony danych osobowych.

Systematyczne planowanie i przeprowadzanie sprawdzeń oraz sporządzanie sprawozdań dla administratorów danych lub GIODO (na podstawie art. 19b uodo) pozwala wykształcić właściwe standardy w zakresie bieżącego, rzetelnego nadzoru nad przestrzeganiem przepisów dotyczących ochrony danych osobowych. Zatem mimo że obowiązki te są obecnie często krytycznie oceniane przez podmioty do nich zobowiązane (chodzi w szczególności o sprawdzenia przeprowadzane na zlecenie GIODO), niewątpliwie służą one zdobywaniu przez ABI cennych doświadczeń i wiedzy. Realizacja tych obowiązków przyczynia się również do upowszechniania znajomości wymogów prawnych

i standardów dotyczących ochrony danych osobowych wśród wszystkich osób mających do czynienia z przetwarzaniem danych osobowych w danej instytucji lub przedsiębiorstwie. Tym samym skorzystanie przez administratorów danych z uprawnienia do powołania ABI oraz realizowanie przez ABI jego zadań przewidzianych w krajowych przepisach o ochronie danych osobowych przyczynia się do podniesienia efektywności systemu ochrony danych osobowych w Polsce oraz stanowi potrzebny i ważny etap przygotowawczy na drodze do właściwego wdrożenia przepisów rozporządzenia ogólnego.

Monika Młotkiewicz – zastępca dyrektora Departamentu Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych.

Rozdział IV
Zadania inspektorów ochrony danych w świetle nowych obowiązków administratorów danych

Do jednych z najdalej idących zmian wprowadzonych rodo należy nadanie nowego statusu ABI (przyszłemu inspektorowi ochrony danych). Dotychczasowe akty prawne nie przyznawały ABI wystarczającej gwarancji niezależności, niezbędnej do swobodnego podejmowania przez nich działań mających bezpośredni wpływ na ochronę danych osobowych, a nawet szerzej – na ochronę prywatności. Dyrektywa 95/46/WE wskazywała jedynie, że osoba odpowiedzialna za ochronę danych musi mieć możliwość wykonywania swoich funkcji w sposób całkowicie niezależny. Rodo – oprócz ogólnego wymogu takiej niezależności – przyznało wprost instrumenty gwarantujące inspektorom ich niezależność. Istotą przyznania takiego statusu inspektorom ochrony danych nie jest jednak wyłącznie podkreślenie ich ważnej roli w procesie ochrony danych osobowych, ale owa niezależność stanowi jeden z instrumentów zapewniających im możliwość pełnego i skutecznego wykonywania zadań. Nie ulega bowiem wątpliwości, że w ślad za poszerzeniem zakresu obowiązków nakładanych na administratorów danych osobowych oraz podmioty przetwarzające dane dojdzie do poszerzenia obowiązków samych inspektorów ochrony danych. Ogólny katalog zadań inspektorów ochrony danych wskazany został w art. 39 rodo i obejmuje: informowanie administratora danych, monitorowanie przestrzegania ogólnego rozporządzenia, pełnienie funkcji punktu kontaktowego, udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz współpracę z organem nadzorczym. Wskazany katalog zadań powinien być jednak oceniany wyłącznie w charakterze katalogu ogólnych form działań podejmowanych przez inspektora ochrony danych, który, mówiąc najogólniej, ma wspierać administratora danych bądź podmiot

przetwarzający dane w wykonywaniu przez niego zadań przewidzianych w ogólnym rozporządzeniu.

Wskazanie, jakie są w istocie zadania przyszłego inspektora ochrony danych wymaga wzięcia pod uwagę wszystkich obowiązków nałożonych przez rodo na administratorów danych oraz udzielenia odpowiedzi na dwa podstawowe pytania. Pierwszym z nich jest pytanie o to, które z obowiązków wynikających z rodo adresowane są wprost do administratora danych lub podmiotu przetwarzającego dane. Drugim – czy możliwe jest, by inspektor ochrony danych wspierał administratora lub przedmiot przetwarzający w realizacji tych obowiązków. Trzeba przy tym pamiętać, że ochrona danych osobowych jest jednym z praw podstawowych przewidzianych Kartą Praw Podstawowych. Dlatego też Trybunał Sprawiedliwości UE w swoim orzecznictwie wielokrotnie podkreślał, że biorąc pod uwagę cel aktów unijnych, polegający na zapewnieniu ochrony podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do prywatności w zakresie przetwarzania danych osobowych, nie można przyjmować wykładni zawężającej (zob. wyrok TSUE w sprawie C 131/12 z 13 maja 2014 r. w sprawie Google Spain pkt 53). Stosując powyższą wykładnię, stwierdzić należy, że inspektor ochrony danych powinien wspierać administratora danych osobowych we wszystkich czynnościach, w których z uwagi na charakter podejmowanych działań jest to możliwe.

Nie we wszystkich przypadkach podjęcie takich działań przez inspektora ochrony danych będzie bowiem możliwe. W szczególności konieczne jest zaakcentowanie, że przepisy rodo wyłączają możliwość przeniesienia na inspektora ochrony danych ciężaru podejmowania decyzji, który wprost nałożony został na administratorów danych lub podmioty przetwarzające. Przykładem mogą być decyzje co do wdrażanych technicznych i organizacyjnych środków ochrony danych osobowych. Artykuł 24 rodo wskazuje wprost, że uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym

prawdopodobieństwie i wadze zagrożenia, to administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rodo. W tym zakresie działania inspektora ochrony danych mogą ograniczyć się wyłącznie do podejmowania działań czysto doradczych, wspierających administratora w podejmowanych przez niego decyzjach.

Wskazanie pozytywnego katalogu wszystkich możliwych zadań nakładanych na przyszłych inspektorów ochrony danych nie jest możliwe. W znacznej części zależą one bowiem od charakteru działalności podejmowanej przez administratora danych bądź podmiot przetwarzający oraz decyzji administratora, w którym ze swoich działań oczekuje wsparcia ze strony inspektora ochrony danych. Administrator może przykładowo oczekiwać od inspektora ochrony danych wsparcia w odbieraniu zgody przez dziecko w przypadku świadczenia przez siebie usług społeczeństwa informacyjnego, ale wyłącznie w przypadku, gdy w ramach prowadzonej przez siebie działalności usługi takie są faktycznie świadczone. Co jednak istotne, rodo poprzez szeroki zakres zadań nałożonych na inspektorów ochrony danych art. 39 rodo wymaga od nich aktywności rozumianej jako inicjowanie działań zmierzających do zapewnienia należytej ochrony danych osobowych.

Możliwe jest natomiast podjęcie próby wskazania tych z zadań, które ciążą na każdym administratorze danych osobowych niezależnie od tego, jaki jest charakter działań, w związku z którymi dane osobowe są przetwarzane. W związku z tymi zadaniami działania inspektorów ochrony danych można podzielić na trzy kategorie. Pierwszą z nich jest wyrażone w art. 39 ust. 1 rodo informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o konkretnych obowiązkach spoczywających na nich na mocy rodo. Drugą jest merytoryczne wsparcie administratora danych, podmiotu przetwarzającego oraz pracowników w podejmowaniu działań zmierzających do zapewnienia zgodnego z prawem przetwarzania danych. Wreszcie trzecim z zadań jest egzekwowanie przestrzegania zasad ochrony danych.

Do zadań, w których realizacji inspektor ochrony danych powinien zawsze wspierać administratora danych osobowych, podejmując wskazane aktywności niezależnie od charakteru prowadzonej przez administratora działalności, należy wykazanie jednej z przesłanek przetwarzania danych osobowych, o których mowa w art. 6–11 rodo. W przypadku gdy podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, inspektor ochrony danych powinien wspierać administratora danych w skonstruowaniu należytego procesu odbierania zgody. Powinien on zagwarantować, że została ona odebrana w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Powyższe dotyczy również respektowania zasad dotyczących przetwarzania danych osobowych, o których mowa w art. 5 rodo. Wskazane zasady stanowić powinny zresztą klucz do podjęcia przez inspektora ochrony danych działań polegających na monitorowaniu przestrzegania rodo, o czym mowa w art. 39 rodo. W związku z ciążącym na administratorze danych obowiązkiem dochowania należytej formy powierzania danych osobowych podmiotowi przetwarzającemu dane do zadań inspektora ochrony danych należeć powinno opiniowanie, a nawet tworzenie w imieniu administratora wzorów umów, odpowiadających wszystkim wymogom przewidzianym w art. 28–29 rodo. Mimo że rodo nie wprowadza wymogu prowadzenia dokumentacji przetwarzania danych osobowych w kształcie przewidzianym w obowiązujących przepisach powszechnie obowiązującego prawa, nakłada na administratora szereg obowiązków dokumentacyjnych. Przykładowo, zgodnie z art. 33 ust. 5 rodo, administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. W praktyce w zdecydowanej większości przypadków wymóg stworzenia oraz aktualizowania takiej dokumentacji ciążył będzie na inspektorze ochrony danych jako na osobie posiadającej największą wiedzę o wszelkich zdarzeniach mogących rodzić ryzyko naruszenia zasad ochrony danych. Nie bez znaczenia pozostaje również wkład inspektorów ochrony danych w zapewnienie należytych środków bezpieczeństwa ochrony danych osobowych. Zgodnie z art. 32

rodo (uwzględniając m.in. stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania), administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne zapewniające należytą ochronę danych osobowych. W praktyce ocena skuteczności zastosowanych środków ochrony oraz rekomendowanie zmian powinno należeć do inspektora ochrony danych. Warto zwrócić uwagę, że powołany przepis wzmacnia stawiany inspektorom ochrony danych osobowych w art. 37 rodo wymóg posiadania kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań. Inspektor ochrony danych powinien być osobą, która poprzez swoje doświadczenie łączy wiedzę o zasadach ochrony danych osobowych z wiedzą o funkcjonowaniu sektora, w ramach którego administrator lub podmiot przetwarzający prowadzą swoją działalność. Bez wątpienia inaczej wyglądają techniki zabezpieczania danych osobowych w sektorze IT wykorzystywane w związku z prowadzeniem archiwów w placówkach medycznych. Z powyższym związane są również przewidziane w art. 25 rodo obowiązek administratora danych uwzględniania ochrony danych w fazie projektowania oraz domyślna ochrona danych. Administrator – uwzględniając: stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych – zobowiązany jest do wdrażania odpowiednich środków technicznych i organizacyjnych podczas określania sposobów przetwarzania oraz w czasie samego przetwarzania. Wskazana zasada, *privacy by design*, nakłada na administratora obowiązek uwzględnienia ochrony danych osobowych już na etapie projektowania rozwiązań technicznych bądź organizacyjnych. O ile działania takie powinny być podejmowane przy wsparciu inspektora ochrony danych, o tyle możliwe jest to wyłącznie w przypadku, gdy posiada on wiedzę pozwalającą mu na rozeznanie się w wykorzystywanych przez administratora technologiach.

Zakres zadań nakładanych na inspektorów ochrony danych w ogólnym rozporządzeniu dalece wykracza poza ich ogólny katalog

wskazany wprost w art. 39 rodo. Żadne z postanowień rodo nie może prowadzić jednak do wniosku o przeniesieniu na inspektorów ochrony danych pełnej odpowiedzialności za podejmowane decyzje, tam gdzie obowiązek wprost nakładany jest na administratora danych lub podmiot przetwarzający.

dr Maciej Kawecki – do 30 października 2016 r. pracownik Departamentu Edukacji Społecznej i Współpracy Międzynarodowej w Biurze GIODO.

Rozdział V
Dokumentacja przetwarzania danych osobowych

Przepisy rodo mają zapewnić nową jakość bezpieczeństwa procesów przetwarzania danych osobowych. Nie zawierają jednak uregulowań, które wprost stanowiłyby o obowiązku prowadzenia dokumentacji przetwarzania danych osobowych w kształcie znanym z obowiązujących obecnie przepisów uodo. Nie oznacza to jednak, że dokumentacja taka nie jest wymagana. Nowe przepisy nakładają bowiem na administratora danych wiele nowych obowiązków, w tym konieczność dokumentowania poniżej opisanych procesów.

Rejestrowanie czynności przetwarzania (art. 30)

- W celu zachowania zgodności z rodo administrator lub podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni.
- Każdy administrator i każdy podmiot przetwarzający zobowiązani są współpracować z organem nadzorczym i na jego żądanie udostępniać mu rejestry w celu monitorowania operacji przetwarzania.

Ocena skutków dla ochrony danych osobowych (art. 35)

- Przed przetwarzaniem danych administrator powinien ocenić jego skutki dla ochrony danych, źródła ryzyka oraz konkretne prawdopodobieństwo i wagę ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania.
- Ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy minimalizowania ryzyka, a także zapewniać ochronę danych osobowych oraz zgodność z przepisami rodo.

Uwzględnianie ochrony danych osobowych w fazie projektowania, domyślna ochrona danych (art. 25)

- Administrator – uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, zagrożenia wynikające z przetwarzania, zarówno przy określaniu sposobów przetwarzania, jak i podczas samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne zapewniające spełnienie wymogów rodo oraz ochronę praw osób, których dane dotyczą (takie jak pseudonimizacja) zaprojektowane w celu skutecznej realizacji zasad ochrony danych (takich jak minimalizacja danych) oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń.
- Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Prawo do ograniczenia przetwarzania (art. 18)

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

- osoba, której dane dotyczą, kwestionuje prawidłowość jej danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych,
- przetwarzanie jest niezgodne z prawem,
- osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
- dane potrzebne są do ustalenia, dochodzenia lub obrony roszczeń osoby, której dane dotyczą, pomimo że administrator nie potrzebuje już tych danych osobowych do celów przetwarzania,

- osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 rodo wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw jej sprzeciwu.

Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19)

- Administrator informuje o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych osobowych – czego dokonał zgodnie z art. 16, 17 ust. 1 i 18 rodo – każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
- Administrator informuje osobę, której dane dotyczą, o odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33)

- Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym: okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta ma umożliwić organowi nadzorczemu na weryfikowanie przestrzegania niniejszego artykułu.

Bezpieczeństwo przetwarzania (art. 32)

- Administrator i podmiot przetwarzający – uwzględniając: stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze ryzyka – wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym:
  - pseudonimizację i szyfrowanie danych osobowych;
  - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

– zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
– regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

- Wywiązywanie się z obowiązków, o których mowa powyżej, można wykazać m.in. poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 rodo, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 rodo.

Wyznaczanie przedstawicieli administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii Europejskiej (art. 27)

- Jeżeli zastosowanie ma art. 3 ust. 2 rodo, to administrator lub podmiot przetwarzający na piśmie wyznacza swojego przedstawiciela w Unii Europejskiej.
- Przedstawiciel zostaje upoważniony przez administratora lub podmiot przetwarzający, by do celów zapewnienia przestrzegania rodo mogły się do niego zwracać – oprócz lub zamiast do administratora lub podmiotu przetwarzającego – w szczególności organy nadzorcze i osoby, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem.

Trudno wyobrazić sobie realizowanie przez administratora obowiązku przestrzegania rodo po 25 maja 2018 r. bez udokumentowania przyjętych wewnętrznych polityk i wdrożonych środków, zgodnych z zasadą uwzględniania ochrony danych, w sytuacji, gdy każdy administrator danych będzie zobowiązany do stworzenia dokumentacji opisującej proces przetwarzania danych osobowych. W celu stworzenia takiej dokumentacji administrator będzie zobowiązany do przeprowadzenia oceny skutków dla ochrony danych, czyli do:

- systematycznego opisywania planowanych operacji przetwarzania danych osobowych i celów przetwarzania,

- oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- oceny, czy planowane operacje przetwarzania są niezbędne oraz proporcjonalne do celów,
- oceny planowanych środków w celu zaradzenia ryzyku, w tym zabezpieczenia, oraz środków i mechanizmów bezpieczeństwa, mających zapewnić ochronę danych osobowych i wykazać przestrzeganie rodo, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, oraz innych osób, których sprawa dotyczy.

Kluczowym elementem systemu ochrony danych osobowych będzie ich administrator. Brak dokumentacji – odzwierciedlającej opis istniejących zagrożeń oraz wdrażanych zabezpieczeń proporcjonalnych do stwierdzonego ryzyka – skutkować może poważną destabilizacją procesów przetwarzania danych i mieć negatywny wpływ na prywatność.

Tomasz Soczyński – zastępca dyrektora Departamentu Informatyki.

Rozdział VI
Inwentaryzacja danych osobowych (lokalny rejestr zbiorów, rejestr czynności i operacji)

Tworząc system zarządzania bezpieczeństwem przetwarzania danych osobowych, należy przeprowadzić inwentaryzację wszystkich aktywów, jakimi dysponuje jednostka, rozumianych jako: informacje i związane z nimi procesy, systemy i sieci teleinformatyczne. Dla bezpieczeństwa danych osobowych – w tym dla zapewnienia, że dane osobowe udostępniane będą wyłącznie osobom do tego uprawnionym – inwentaryzacja taka powinna uwzględniać przyjęte zasady klasyfikacji przetwarzanych informacji. Przepisem rodo zobowiązującym administratorów danych i podmioty przetwarzające do wprowadzenia takiej inwentaryzacji jest art. 30 rodo dotyczący rejestrowania czynności przetwarzania. Przepis ten, podobnie jak obecnie obowiązująca uodo, w szczególnych przypadkach wymaga prowadzenia rejestru czynności przetwarzania danych osobowych. Jego zawartość przypomina rejestr zbiorów danych osobowych, do prowadzenia którego zobowiązani są obecnie ABI. Wprowadzony w rodo tzw. rejestr czynności przetwarzania należy rozumieć jako wykaz przetwarzanych zbiorów danych, na które dzieli się wszystkie przetwarzane u danego administratora danych informacje ze względu na: zakres przetwarzanych danych, cele przetwarzania oraz kategorie odbiorców, którym dane zostają udostępnione.

Za takim rozumieniem pojęcia „czynności przetwarzania" przemawia, wymagany w art. 30 ust. 1 pkt a – pkt g oraz art. 30 ust. 2 pkt a do pkt d rodo opis tych czynności. Z wykazu tego jasno wynika, że przez pojęcie „czynności przetwarzania" nie należy rozumieć poszczególnych etapów przetwarzania danych w ramach danego zbioru – takich jak pozyskiwanie danych, wysyłanie do podmiotów danych określonego rodzaju informacji, usuwanie danych oraz wykonywanie na zgromadzonych danych określonego rodzaju operacji (jak np.

naliczenie zobowiązania podatkowego itp.), lecz wszystkie operacje globalnie na określonym zbiorze danych. Granice takiego zbioru mają być wyznaczane nie przez poszczególne cząstkowe operacje przetwarzania, lecz przez wskaźniki wymienione odpowiednio w art. 30 ust. 1 pkt. a–g i w art. 30 ust. 2 pkt. a–d (takie jak: zakres danych, cel przetwarzania, kategorie ich odbiorców itp.), które pozwalają pogrupować wszystkie przetwarzane przez danego administratora dane w jeden lub kilka zbiorów.

Prowadzenie wspomnianego rejestru czynności przetwarzania nie jest jednak obowiązkiem powszechnym. Zgodnie z art. 30 ust. 5 rodo, do prowadzenia ww. rejestrów zobowiązani są administratorzy i podmioty przetwarzające, którzy zatrudniają 250 lub więcej osób oraz gdy:

- dokonują systematycznego przetwarzania mogącego powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, lub
- dokonują przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub
- przetwarzają dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 rodo.

W rejestrze prowadzonym przez podmioty przetwarzające nie podaje się celu przetwarzania i kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione, oraz planowanych terminów usunięcia poszczególnych kategorii danych.

Artykuł 30 rodo – ze względu na wskazane tam ograniczenia dotyczące obowiązku prowadzenia rejestracji czynności przetwarzania tylko do podmiotów zatrudniających więcej niż 250 osób lub przypadków przetwarzania szczególnych kategorii danych oraz gdy przetwarzanie danych może spowodować duże ryzyko naruszenia praw i wolności – należy traktować jako wymaganie minimalne w tym zakresie. Prowadzenie ww. rejestru nie zwalnia z prowadzenia innych ewidencji przetwarzanych aktywów, jeśli wynika to z analizy zagrożeń lub z zastosowanej metodyki budowy systemu zarządzania bezpieczeństwem informacji.

Wykaz informacji zawartych w rejestrze czynności przetwarzania

Lp.	Zawartość rejestru czynności przetwarzania prowadzonego przez administratora danych	Zawartość rejestru czynności przetwarzania prowadzonego przez podmiot przetwarzający
1.	imię i nazwisko lub nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych	imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych
2.	cele przetwarzania	
3.	opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	kategorie przetwarzań dokonywanych w imieniu każdego z administratorów
4.	kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
5.	gdy ma to zastosowanie – informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń	gdy ma to zastosowanie – informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń
6.	jeżeli jest to możliwe – planowane terminy usunięcia poszczególnych kategorii danych	
7.	jeżeli jest to możliwe – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 rodo	jeżeli jest to możliwe – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 rodo

dr inż. Andrzej Kaczmarek – dyrektor Departamentu Informatyki.

Rozdział VII
Sprawdzenia zlecane ABI przez GIODO na tle dotychczasowych doświadczeń

Wraz z wejściem w życie z początkiem 2015 r. znowelizowanych przepisów uodo, GIODO zyskał nowe, dodatkowe narzędzie, wprowadzone w dodanym do uodo art. 19b; umożliwia ono realizację uprawnień kontrolnych wobec podmiotów przetwarzających dane osobowe. Na mocy wskazanego przepisu GIODO może teraz w wykonaniu przyznanego uprawnienia zwrócić się do ABI wpisanego do stosownego rejestru o dokonanie sprawdzenia u administratora danych, który powołał ABI, wskazując zakres i termin sprawdzenia.

Dotychczas organ do spraw ochrony danych osobowych był wyposażony w środki kontrolne wynikające z art. 14 uodo, umożliwiające przede wszystkim przeprowadzenie odpowiednich czynności inspekcyjnych w miejscu przetwarzania danych osobowych. Mając prawo wstępu do pomieszczeń, w których zlokalizowany jest zbiór danych (lub dane przetwarzane poza zbiorem), GIODO mógł m.in. żądać złożenia pisemnych lub ustnych wyjaśnień, wzywać i przesłuchiwać w charakterze świadka, dokonywać oględzin (urządzeń, nośników, systemów informatycznych) oraz mieć wgląd do danych i dokumentów. Kontrole przeprowadzane na podstawie wskazanych uprawnień odbywały się w miejscu prowadzenia działalności lub wykonywania publicznych obowiązków przez administratorów danych lub podmioty przetwarzające dane na podstawie powierzenia, o którym mowa w art. 31 uodo; niekiedy osoby reprezentujące te podmioty składały wyjaśnienia (zeznania) w Biurze GIODO.

Jak wskazuje się w piśmiennictwie, jednym z kryteriów podziału kontroli na różne jej rodzaje jest sposób prowadzenia kontroli: pośrednio lub bezpośrednio. I tak: „Kontrola bezpośrednia polega na obserwowaniu i ocenie działalności podmiotu kontrolowanego w miejscu, gdzie działalność jest prowadzona (stąd określa się ją także mianem kontroli na miejscu)". Istotą kontroli pośredniej jest sprawdzenie i ocena działalności podmiotu kontrolowanego w oparciu o analizę dokumentów (np. sprawozdań) dostarczonych

przez podmiot kontrolowany. Tego rodzaju kontrola dokonywana jest zazwyczaj w siedzibie podmiotu prowadzącego kontrolę i dlatego określa się ją mianem „kontroli siedzącej" bądź „kontroli kameralnej"[1].

Wprowadzona nowelizacja stworzyła możliwość skontrolowania podmiotów przetwarzających dane osobowe bez konieczności udawania się na miejsce ich aktywności lub wzywania ich do siedziby GIODO, lecz poprzez prowadzenie na odległość stosownej korespondencji. Uprawnienie, które zyskał GIODO, polegające na skierowaniu wystąpienia o dokonanie sprawdzenia, należałoby zatem zakwalifikować jako kontrolę pośrednią, mającą właśnie „siedzący", „kameralny" charakter.

Do czasu wprowadzenia omawianych przepisów GIODO miał również legitymację do weryfikowania na odległość kwestii dotyczących zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych poprzez prowadzenie postępowania wyjaśniającego na zasadzie kierowania pisemnych zapytań i wymiany korespondencji w tym zakresie. Jednak proces ten nie był sformalizowany w sposób, w jaki może się to odbywać obecnie, przy zastosowaniu narzędzia, jakim jest sprawdzenie. Po pierwsze, uodo wskazuje, do kogo GIODO może zwrócić się z wnioskiem o dokonanie sprawdzenia i co takie wystąpienie powinno zawierać. Po drugie, GIODO określa formę, zawartość, sposób sporządzenia i przekazania organowi wyników przeprowadzonego sprawdzenia.

Jak wynika z art. 19b ust. 1 uodo, GIODO, wybierając ten rodzaj kontroli i kierując do ABI wystąpienie o dokonanie sprawdzenia, jest obowiązany wskazać jego zakres i termin. A zatem powinien określić, jakie kategorie danych oraz jakie procesy przetwarzania danych (czy np. tylko zbieranie, czy też przechowywanie, archiwizowanie, udostępnianie lub usuwanie) mają takiemu sprawdzeniu podlegać, a także wyznaczyć termin dokonania sprawdzenia. Sprawdzenie może być skierowane wyłącznie do ABI zgłoszonego przez administratora danych, który go powołał, do ogólnokrajowego, jawnego rejestru ABI prowadzonego przez GIODO na podstawie art. 46c uodo. Z kolei po stronie ABI istnieje w takiej sytuacji

1 P. Fajgielski, *Kontrola i audyt przetwarzania danych osobowych*, wyd. I, Wrocław 2010.

obowiązek przedstawienia – po dokonaniu sprawdzenia – GIODO, za pośrednictwem administratora danych, sprawozdania, którego elementy zostały określone w art. 36c uodo.

Co bardzo istotne, w myśl art. 19b ust. 3 uodo, dokonanie przez ABI sprawdzenia nie wyłącza prawa Generalnego Inspektora do przeprowadzenia kontroli na dotychczasowych zasadach, czyli na podstawie przepisów, które obowiązywały, zanim wprowadzono instytucję sprawdzenia. Inspektorzy upoważnieni przez GIODO mogą zatem udać się do podmiotu poddanego sprawdzeniu w celu zweryfikowania przedstawionego sprawozdania ze sprawdzenia lub dokonania dodatkowych ustaleń dotyczących stanu faktycznego.

Kierując wystąpienie o dokonanie sprawdzenia, organ do spraw ochrony danych osobowych wskazuje zakres sprawdzenia w możliwie najbardziej szczegółowy sposób. Poza określeniem przedmiotu (kategorii danych, procesów przetwarzania danych) określa także, jakiego rodzaju dowody powinny zostać załączone do sprawozdania w celu potwierdzenia twierdzeń w nim zawartych.

Jak wynika z dotychczasowych doświadczeń[2], jakość sprawdzenia i opracowanego na jego podstawie sprawozdania zależy w znacznym

2 GIODO w 2015 r. wystosował 13 wystąpień o dokonanie sprawdzenia, na zasadach określonych w art. 19b uodo. Pierwsze wystąpienie przesłano do Rzecznika Praw Obywatelskich, wskazując jako zakres sprawdzenia sposób przetwarzania danych osobowych przy użyciu monitoringu wizyjnego stosowanego w Biurze Rzecznika Praw Obywatelskich. Kolejne zostały skierowane do 10 wytypowanych banków i objęły zakresem kwestie zabezpieczenia danych osobowych klientów tych instytucji finansowych.
W 2016 r. GIODO postanowił dokonać sprawdzeń w trzech obszarach: przetwarzania przez banki danych osobowych w celach marketingowych oraz rozpatrywania sprzeciwów, o których mowa w art. 32 ust. 1 pkt 8 ustawy uodo; przetwarzania przez towarzystwa ubezpieczeniowe danych o stanie zdrowia, w związku z oferowaniem ubezpieczeń zdrowotnych; realizacji przez gminy obowiązków informacyjnych, o których mowa w art. 24 i art. 33 uodo. Do banków zostało skierowanych 20 wystąpień o dokonanie sprawdzenia, zaś do towarzystw ubezpieczeniowych – 10 wystąpień, a kolejnych 15 do gmin.

stopniu od kompetencji ABI. Im większym doświadczeniem dysponuje ABI i im większą ma wiedzę, tym sprawniej przebiega proces oceny sprawozdania dokonywanej przez GIODO. Wówczas nie ma potrzeby prowadzenia dodatkowej korespondencji w celu doprecyzowania sprawozdania lub przedstawiania dodatkowych dowodów, zwłaszcza że z wniosku o dokonanie sprawdzenia jednoznacznie wynika, jakie informacje powinny się w sprawdzeniu znaleźć. Natomiast niewystarczająca wiedza ABI w odniesieniu do przepisów o ochronie danych osobowych może skutkować koniecznością wyjaśniania przez organ, np. jakich elementów brakuje w sprawozdaniu lub w jaki sposób powinny zostać poczynione ustalenia dotyczące stanu faktycznego, a także wskazywania na właściwe rozumienie przepisów, których sprawdzenie dotyczy. Brak wyczerpującego opisu stanu faktycznego lub załączenia stosownych dowodów uniemożliwia bowiem GIODO dokonanie prawidłowej oceny przedłożonego przez ABI sprawozdania.

Z powyższych powodów sprawdzenie daje możliwość weryfikacji stanu faktycznego w trochę inny sposób niż kontrole prowadzone na „tradycyjnych" zasadach. Opiera się bowiem tylko na materiale dowodowym przedstawionym przez ABI, bez bezpośredniego dokonania czynności przez inspektorów, takich jak np. oględziny miejsca przechowywania danych i oględziny systemów informatycznych. Poza tym z jednej strony pozwala na skontrolowanie na odległość, bez potrzeby udawania się na miejsce, wybranych obszarów przetwarzania danych osobowych i w dużo większej liczbie podmiotów, niż jest to możliwe w ramach dotychczas prowadzonych inspekcji. Z drugiej jednak strony ocena sprawozdania dokonywana w sytuacji, gdy zachodzi konieczność prowadzenia dodatkowej korespondencji, wymaga często znacznie więcej czasu.

W związku z wejściem w życie rodo modyfikacji ulegnie zakres uprawnień GIODO. Nie budzi wątpliwości, że organowi do spraw ochrony danych osobowych, zwanemu w rodo „organem nadzorczym", nadal będzie przysługiwało prawo kontrolowania podmiotów przetwarzający dane osobowe, polegające w szczególności na:

– nakazywaniu administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań, oraz
– prowadzeniu postępowań w formie audytów ochrony danych,
– uzyskiwaniu od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań,
– uzyskiwaniu dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego (art. 58 ust. 1 lit. a, b, e i f rodo).

Jednocześnie, jak wynika z art. 58 ust. 6 rodo, każde państwo członkowskie może przewidzieć w swoich przepisach, że jego organowi nadzorczemu będą przysługiwały – poza wymienionymi w art. 58 ust. 1, 2 i 3 rodo – także inne uprawnienia, z tym że ich wykonywanie nie może utrudniać skutecznego stosowania przepisów rozdziału VII rodo. Zatem teraz, gdy rozpoczęto prace legislacyjne nad ukształtowaniem odpowiednich krajowych przepisów o ochronie danych osobowych, które zastąpią regulacje dotychczas obowiązujące, od prawodawcy zależy, w jaki sposób określi uprawnienia kontrolne GIODO. Po udzieleniu w pierwszej kolejności odpowiedzi na pytanie, czy w ogóle na gruncie rodo jest możliwe wprowadzenie w polskim ustawodawstwie przepisów uprawniających do zlecania przez organ nadzorczy dokonywania sprawdzeń, konieczne będzie podjęcie decyzji, czy wyodrębnianie takiego szczególnego uprawnienia jest konieczne. Rodo daje bowiem organowi do spraw ochrony danych osobowych cały szereg nowych uprawnień służących kontroli przestrzegania przepisów prawa. Po przeprowadzeniu stosownej analizy w omawianym zakresie może okazać się, że nie będzie już miało miejsca wykonywanie sprawdzeń na takich zasadach, z jakimi teraz mamy do czynienia.

Katarzyna Hildebrandt – zastępca dyrektora Departamentu Inspekcji.

Gdzie szukać pomocnych informacji?

Rozpoczęcie stosowania rodo to duże wyzwanie dla wszystkich, których prawa i obowiązki akt ten reguluje. W wielu przypadkach będziemy mieć do czynienia z instytucjami prawnymi dotąd nieznanymi sektorowi ochrony danych, a także ze znacznymi modyfikacjami istniejących rozwiązań prawnych.

Rodo zawiera wiele zwrotów niedookreślonych i klauzul generalnych, które wymagać będą wykładni treści przepisów w konkretnych sytuacjach związanych z przetwarzaniem danych osobowych. Nadanie rodo takiej treści było działaniem świadomym. Miało ono zapewnić normom rodo aktualność, niezależnie od ciągłego rozwoju nowych technologii. Niemniej dla adresatów tych norm przyjęcie powyższej konstrukcji będzie oznaczać konieczność dokonywania wykładni użytych pojęć poprzez rozkodowanie zawartych w przepisach treści prawnych.

Warto więc wskazać na źródła informacji pomocnych w dokonywaniu takiej wykładni. Bez wątpienia pierwszym z nich są opinie wydawane przez Grupę Roboczą Art. 29, a po rozpoczęciu stosowania rodo – jej następcę prawnego, Europejską Radę Ochrony Danych. Opinie takie z pewnością będą przez Grupę tworzone oraz udostępniane na jej stronie (http://ec.europa.eu/justice/data-protection/article-29/index_en.htm), w zakładce „Opinie i rekomendacje". Ponadto opinie te, po ich przetłumaczeniu na język polski, GIODO, będzie, jak dotąd, udostępniał na swojej stronie internetowej.

Kolejnym źródłem informacji jest strona internetowa GIODO (www.giodo.gov.pl) oraz strony WWW organów nadzorczych z innych państw członkowskich UE. Zamieszczane są na nich obowiązujące w dziedzinie ochrony danych osobowych przepisy prawa, a także informacje i wskazówki dotyczące ich wykładni. Często można na nich znaleźć informacje o wydarzeniach dotyczących unijnej reformy ochrony danych osobowych, takich jak warsztaty, konferencje i szkolenia.

Na stronie internetowej GIODO w zakładce Prawo znajdują się zarówno informacje dotyczące reformy ochrony danych osobowych (w sekcji

Reforma ochrony danych osobowych), jak i treść nowych przepisów rodo (w sekcji Przepisy prawa | Europejskie | Rozporządzenia). W tej samej zakładce dostępne są też pozostałe, obowiązujące w zakresie ochrony danych osobowych akty prawne (krajowe, europejskie i międzynarodowe). Na stronie tej znaleźć można ponadto wykaz literatury fachowej oraz informacje o wyrokach sądów polskich i zagranicznych. Materiały są na bieżąco aktualizowane i rozszerzane, a wyszukiwanie informacji ułatwia zamieszczona na stronie wyszukiwarka.

Wiele pomocnych informacji dotyczących powołania administratorów bezpieczeństwa informacji i wykonywania przez nich zadań na podstawie obowiązujących przepisów krajowych dostępnych jest w serwisie ABI-Informator (https://abi.giodo.gov.pl).

Wykładnia przepisów rodo może okazać się łatwiejsza po wydaniu przez Komisję Europejską aktów wykonawczych oraz aktów delegowanych, które uzupełniają (wykonują) postanowienia rodo. Ich celem jest ponadto ujednolicenie stosowania rodo w poszczególnych państwach członkowskich. Komisja będzie jednak uprawniona do wydania takich aktów dopiero po rozpoczęciu stosowania rodo, a więc po 25 maja 2018 r.

Poza powyższymi źródłami informacji okazją do poszerzania wiedzy i wymiany wzajemnych doświadczeń mogą być również szkolenia sektorowe organizowane przez GIODO. Szkolenia takie adresowane są do ABI i mają w założeniu ułatwić prawidłowe realizowanie obecnych i przyszłych obowiązków administratorów danych i wspierających ich ABI w określonych dziedzinach działalności. Informacje o szkoleniach przekazywane są administratorom danych, którzy zgłosili powołanie ABI do rejestru prowadzonego przez GIODO, a także za pośrednictwem strony internetowej www.giodo.gov.pl.

Monika Młotkiewicz, dr Maciej Kawecki