

Współpraca ABI i GIODO

– perspektywy rozwoju



Monika Młotkiewicz
Radca prawny, zastępca dyrektora Departamentu
Rejestracji ABI i Zbiorów Danych Osobowych
w Biurze GIODO

Dzięki harmonijnej współpracy GIODO i ABI – przyszłych inspektorów ochrony danych osobowych możliwe jest stworzenie skutecznego systemu ochrony danych osobowych. Zwornikiem nowego, odpowiadającego wyzwaniom XXI wieku i jednolitego dla całej Unii Europejskiej, systemu ochrony danych osobowych, tworzonego na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE; dalej: RODO, mają być z jednej strony inspektorzy ochrony danych – obecni ABI, z drugiej zaś organy nadzorcze – w Polsce Generalny Inspektor Ochrony Danych Osobowych. Podmioty te – przepisami powołanego rozporządzenia – zostały zobowiązane do wzajemnej pomocy i współpracy, co w założeniu ma im ułatwić wywiązywanie się ze swoich obowiązków.

Współpraca w zakresie monitorowania stosowania przepisów

Ogólne rozporządzenie o ochronie danych tworzy nowe płaszczyzny współpracy inspektorów ochrony danych (obecnych ABI) i organu nadzorczego, tj. Generalnego Inspektora Ochrony Danych Osobowych (GIODO). Jednak w Polsce zaczątków systemu, w którym nad zgodnością przetwarzania danych osobowych z prawem czuwać ma nie tyl-

ko GIODO, ale też powoływani przez administratorów danych ABI, można upatrywać w obowiązującym do początku 2015 r. art. 36 ust. 3¹ ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 poz. 922, dalej: OchrDanychU). Dzięki nowelizacji ustawy o ochronie danych osobowych, wprowadzonej ustawą z 7.11.2014 r. o ułatwieniu wykonywania działalności gospodarczej, od 1.1.2015 r. zadania ABI zostały rozbudowane i ukształtowane w sposób mający zapewnić bieżące monitorowanie na poziomie we-

wnętrznym przestrzegania przepisów o ochronie danych osobowych u tych administratorów danych, którzy zdecydowali się na powołanie ABI. Zadanie to jest realizowane m.in. przez dokonywanie sprawdzeń dla administratorów danych (w tym na zlecenie GIODO) i sporządzanie z nich sprawozdań oraz nadzorowanie wdrożenia wymaganej przepisami dokumentacji.

¹ Zgodnie z art. 36 ust. 3 OchrDanychU do 1.1.2015 r., „Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w art. 36 ust. 1, chyba że sam wykonuje te czynności”.

Dzięki temu ABI zdobywają wartościowe doświadczenia w zakresie monitorowania zgodności z przepisami prawa działań podejmowanych przez administratorów danych oraz weryfikowania skuteczności stosowanych narzędzi i procedur. Uczą się rzetelnego i obiektywnego „zbierania dowodów”, które potwierdzają należyte przestrzeganie przepisów, lub wskazują wymagające usunięcia nieprawidłowości. Dla podnoszenia kompetencji w tym zakresie szczególnie przydatne są sprawdzenia dokonywane na zlece-

nie GIODO, ponieważ wówczas sposób przeprowadzenia sprawdzenia jest weryfikowany przez inspektorów GIODO. W przypadku tzw. sprawżeń sektorowych, dotyczących przetwarzania danych w określonej branży, na podstawie przekazanych przez ABI sprawozdań, GIODO opracowuje zestawienia wniosków², w których zawarta jest uogólniona ocena poddane go sprawdzeniom zakresu zagadnień oraz w których wskazuje się błędy popełniane przez ABI przy wykonywaniu zleconych sprawżeń.

lu przypadkach powinny być dokumentowane.

Kary administracyjne

Tak jak obecnie, również na gruncie RODO, organ nadzorczy będzie mógł kontrolować przestrzeganie przepisów związanych z wyznaczeniem inspektora ochrony danych i zapewnieniem mu przez administratora danych (od 25.5.2018 r. również przez podmiot przetwarzający) odpowiednich warunków pozwalających na niezależne wykonywanie zadań. Stosownie do art. 83 ust. 5 RODO, naruszenia wszystkich przepisów bezpośrednio odnoszących się do inspektorów ochrony danych osobowych (art. 37–39 RODO) podlegają administracyjnej karze pieniężnej nałożonej przez GIODO. Karami tymi obwarowane są zatem zarówno poszczególne obowiązki administratorów danych i podmiotów przetwarzających dotyczące wyznaczania inspektora ochrony danych i zapewnienia mu określonych warunków wykonywania funkcji, jak i wykonywanie zadań przez inspektorów ochrony danych.

Najczęściej popełniane błędy	
1.	Brak wszystkich niezbędnych informacji (odniesienia się do pytań zawartych w wystąpieniu GIODO).
2.	Brak dowodów potwierdzających dokonane ustalenia.
3.	Brak spójności pomiędzy ustaleniami a załącznikami.
4.	Brak wskazania, które z załączonych dokumentów dotyczą poszczególnych ustaleń.
5.	Brak wskazania planowanych lub podjętych działań przywracających stan zgodny z prawem (art. 36c pkt 7 OchrDanychU).
6.	Przesłanie sprawozdania bez wymaganego pośrednictwa administratora danych (brak podpisu administratora danych na sprawozdaniu lub w piśmie przewodnim – art. 19b ust. 2 OchrDanychU).
7.	Brak podpisu ABI lub brak jego parafy na każdej stronie sprawozdania (art. 36c pkt 9 OchrDanychU).

Wysiłek wkładany obecnie – z jednej strony przez ABI – w przeprowadzanie sprawżeń na podstawie art. 19b OchrDanychU oraz – przez pracowników GIODO z drugiej strony – w weryfikowanie sprawżeń i sporządzanie raportów zestawiających wyniki sprawżeń, jest efektywnym poligonem współpracy tych podmiotów. Praktyka w zakresie dokonywania szczegółowych ustaleń oraz ich dokumentowania może przełożyć się na umiejętności wymagane od inspektorów na gruncie RODO, zwłaszcza w kontekście zasady rozliczalności wyrażonej w art. 5 ust. 2. Należy zatem założyć, że doświadczenia zdobywane dzięki sprawdzeniom mogą okazać się bardzo pomocne po wejściu do stosowania RODO, tym bardziej że zgodnie z art. 39 ust. 1 RODO,

zadaniem inspektora ochrony danych będzie monitorowanie przestrzegania przedmiotowego rozporządzenia, innych przepisów UE lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych. Zgodnie z Wytocznymi Grupy Roboczej Art. 29 dotyczącymi inspektorów ochrony danych³, na wykonanie tego obowiązku składać się mogą m.in. następujące czynności: zbieranie informacji w celu identyfikacji procesów przetwarzania; analizowanie i sprawdzanie zgodności tego przetwarzania; informowanie, doradzanie i rekomendowanie określonych działań administratorowi albo podmiotowi przetwarzającemu. Ze względu na zasadę rozliczalności działania te w wie-

Przeprowadzanie kontroli GIODO

Przeprowadzanie kontroli GIODO to obszar, w którym przedstawiciele organu i inspektorzy współdziałają obecnie w sposób bezpośredni. Przed rozpoczęciem kontroli inspektorzy GIODO sprawdzają, czy administrator danych powołał ABI i jeśli tak, to dokonują czynności kontrolnych, współpracując z tym właśnie fachowym podmiotem. W czasie kontroli ABI udziela inspektorom GIODO niezbędnej po-

² Zestawienie wyników sektorowych sprawżeń zgodności przetwarzania danych z przepisami o ochronie danych osobowych, które zostały przeprowadzone przez administratorów bezpieczeństwa informacji w bankach w zakresie marketingu kierowanego do klientów oraz osób niebędących klientami banków dostępne jest na stronie www.giodo.gov.pl w zakładce kontrole (http://www.giodo.gov.pl/1520252/id_art/9848/j/pl/0).

³ Wytocznice dotyczące inspektorów ochrony danych („DPO”) przyjęte 13.12.2016 r. (ostatnio zmienione i przyjęte 5.4.2017 r.) http://www.giodo.gov.pl/1520282/id_art/9740/j/pl/.

mocy, dostarczając na bieżąco koniecznych informacji. Czasem ABI reprezentuje administratora w czasie czynności pokontrolnych, np. jako jego pełnomocnik.

Współpraca taka była i jest w interesie obu stron. Po wejściu do stosowania nowych unijnych przepisów stanie się ona ponadto ich prawnym obowiązkiem. Zgodnie bowiem z art. 39 ust. 1 lit. d i e RODO, inspektor ochrony danych (DPO) powinien „współpracować z organem nadzorczym” i „pełnić funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzić konsultacje we wszelkich innych sprawach”. Jak we wspomnianych wytycznych wskazuje Grupa Robocza Art. 29, inspektor ma pełnić funkcję punktu kontaktowego, „by umożliwić organowi nadzorczemu dostęp do dokumentów i informacji w celu realizacji zadań, o których mowa w art. 57 RODO, jak również wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, zgodnie z art. 58 RODO”. W przypadku zgłoszenia naruszenia ochrony danych przez administratora organowi nadzorczemu, administrator jest zobowiązany do podania danych kontaktowych DPO, w celu uzyskania przez organ wszelkich ważnych w tej sprawie informacji.

Ważne

W kontekście zasady rozliczalności i podejścia opartego na ryzyku warto dodać, że RODO zakłada dużo większą samodzielność i odpowiedzialność zarówno administratorów danych i podmiotów przetwarzających, jak i inspektorów ochrony danych.

Wprowadzie również obecnie, zgodnie z art. 36 OchrDanychU, administratorzy danych mają obowiązek przyjęcia środków, które zapewnią poziom bezpieczeństwa odpowiedni do kategorii danych i zagrożeń, niemniej większość podmiotów podchodzi do ochrony danych osobowych jedynie jako do formalnego, jednorazowo spełnianego obowiązku, ograniczającego się do opracowania polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym. Nader często zdarza się, że dokumenty te nie są nawet rozpowszechnione i wprowadzone w życie w danej organizacji. Bywa, że nie są także aktualizowane odpowiednio do zmieniających się warunków przetwarzania.

Zasada rozliczalności i *risk based approach*

Taka postawa nie będzie już możliwa po rozpoczęciu stosowania RODO. Wprowadzając zasadę rozliczalności i *risk based approach*, nowa regulacja wymusi podejście odpowiedzialne i efektywne. Konieczne będzie dokonywanie faktycznych, zindywidualizowanych ocen procesów przetwarzania i związanych z nimi ryzyk oraz dobieranie do nich odpowiednich mechanizmów, polityk i procedur, które następnie będą musiały być na bieżąco monitorowane, weryfikowane i uaktualniane. To spowoduje, że zarówno administratorzy danych i wspierający ich inspektorzy danych, jak i inspektorzy organów nadzorczych, nie będą mogli posługiwać się jednym uniwersalnym wykazem „wymogów do spełnienia”. Inspektorzy organu nadzorczego będą musieli brać pod uwagę różnorodność praktyk i zastosowanych rozwiązań oraz środków technicznych i organizacyjnych, co będzie powodowało, że zanim organ rozwiązania te oceni (m.in. podczas czynności kontrolnych), będzie musiał je dobrze

przeanalizować. Narzędziem, które będzie ułatwiać organowi nadzorczemu efektywne wypełnianie jego obowiązków kontrolnych, będą ponadto rejestry **czynności przetwarzania danych osobowych i rejestry kategorii czynności przetwarzania danych dokonywanych w imieniu administratora**. Jak wskazuje Grupa Robocza Art. 29 w Wytycznych dotyczących inspektorów ochrony danych, obecnie często to inspektor ochrony danych tworzy i prowadzi powyższe rejestry na podstawie danych otrzymanych od pozostałych komórek organizacji. Ze względu na swoją zawartość rejestry są też pomocnym narzędziem dla inspektora ochrony danych w stosowaniu zasady rozliczalności, zapewnianiu przestrzegania RODO oraz prowadzeniu prawidłowej polityki w zakresie ochrony danych⁴.

Współpraca w zakresie oceny skutków dla ochrony danych i uprzednich konsultacji

Ocena skutków dla ochrony danych oraz będąca jej elementem ocena ryzyka naruszenia praw i wolności osób fizycznych jest jednym z ważniejszych nowych obowiązków związanych z wdrożeniem RODO. Obowiązkiem, którego realizacja oraz egzekwowanie mogą okazać się w praktyce dużym wyzwaniem. Przeprowadzenie oceny skutków dla ochrony danych jest – w świetle art. 35 pkt 3a RODO – obowiązkowe 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

⁴ Art. 30 ust. 4 w zw. z art. 31 rozporządzenia ogólnego o ochronie danych – każdy administrator i każdy podmiot przetwarzający zobowiązani są współpracować z organem nadzorczym i na jego żądanie udostępniać mu rejestry w celu monitorowania operacji przetwarzania.

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. 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”. Wniosek o rozpoczęcie uprzednich konsultacji ma zawierać dane kontaktowe inspektora ochrony danych, jeżeli został wyznaczony, ponieważ inspektor ochrony danych (co z kolei wynika z katalogu jego obowiązków) ma pełnić rolę punktu kontaktowego dla organu nadzorczego, a zatem „fachowego źródła informacji”. Jest to uzasadnione tym, że dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony (art. 35 ust. 2 RODO) i ta konsultacja, jak również podjęta decyzja, powinna zostać udokumentowana w przeprowadzonej ocenie skutków dla ochrony danych (DPIA)⁵. Inspektor ochrony danych (DPO) powinien również monitorować wykonanie DPIA.

Natomiast GIODO w zakresie oceny skutków dla ochrony danych (tak jak każdy inny organ nadzorczy w Unii Europejskiej) zobowiązany został do prowadzenia wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania takiej oceny oraz udzielania pisemnych zaleceń w sytu-

acjach wskazanych w art. 36 RODO. Pomocnymi instrumentami w zakresie dokonywania oceny skutków dla ochrony danych mają być również wydawane przez organy nadzorcze oraz Europejską Radę Ochrony Danych Osobowych (która po 25.5.2018 r. ma zastąpić Grupę Roboczą Art. 29) wskazówki i wytyczne, a także zatwierdzane przez organ nadzorczy branżowe kodeksy postępowania.

Działania edukacyjne i wymiana informacji

Bardzo doniosłą i ważną sferą wspólnych działań inspektorów ochrony danych i organów nadzorczych jest podnoszenie poziomu świadomości prawnej, edukowanie osób zaangażowanych w przetwarzanie danych osobowych i odpowiedzialnych za wykonywanie obowiązków w tym zakresie. Na mocy obecnie obowiązujących przepisów jest to jedno z zadań ABI (zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych). Inspektor ochrony danych zaś, zgodnie z art. 39 ust. 1 lit. a RODO, ma informować i doradzać w zakresie obowiązków ciążyących na administratorze, podmiocie przetwarzającym i pracownikach. Prawidłowe wykonywanie obowiązków doradczych i edukacyjnych bezpośrednio przekłada się na podejmowanie przez administratorów danych i podmioty przetwarzające świadomych i trafnych decyzji. Zatem tak jak teraz ABI, a w niedalekiej przyszłości inspektorzy ochrony danych będą mieli obowiązek docierać z wiedzą bezpośrednio do osób podejmujących decyzje i przetwarzających dane, tak organy nadzorcze, w tym GIODO, powinny edukować systemowo, poprzez działania o jak najszerszym zasięgu, w tym ogólnokrajowym. Każdy organ nadzorczy na swoim terytorium

ma upowszechniać w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk. Ma też upowszechniać wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy RODO (art. 57 ust. 1). W przypadku GIODO edukowanie podmiotów zobowiązanych do przestrzegania przepisów o ochronie danych osobowych będzie następowało m.in. poprzez dalsze prowadzenie serwisów edukacyjno-informacyjnych (w chwili obecnej są to np. edu-GIODO, ABI-Informator) oraz wydawanie poradników, wytycznych i innych materiałów szkoleniowych. Dużą rolę odgrywać będą wytyczne i rekomendacje Grupy Roboczej Art. 29, a następnie Europejskiej Rady do Spraw Ochrony Danych Osobowych. Inspektorzy wewnątrz organizacji, dla których zostali wyznaczeni, będą mogli natomiast dobierać środki szkoleniowe i komunikacyjne do konkretnych odbiorców. Działania na tych dwóch poziomach będą zatem komplementarne i przez to bardziej skuteczne.

Warto zauważyć, że współpraca GIODO i inspektorów ochrony danych potrzebna będzie również w zakresie objaśniania podmiotom danych, na czym polegają ich uprawnienia wynikające z przepisów prawa oraz jak z nich korzystać. Artykuł 38 ust. 4 RODO bezpośrednio uprawnia osoby, których dane dotyczą, do kontaktowania się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia. Ten akt prawny kładzie bowiem bardzo duży nacisk na urzeczywistnienie praw osób,

⁵ Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko”, do celów rozporządzenia 2016/679 (wersja poddana konsultacjom – nieoficjalne tłumaczenie – http://www.giodo.gov.pl/1520281/id_art/9930/j/pl).

których dane dotyczą i w tym zakresie np. zobowiązuje administratorów danych nie tylko do rzetelnego realizowania uprawnień osób fizycznych, ale do ułatwiania osobom uprawnionym dochodzenia przysługujących im praw⁶.

Natomiast organy nadzorcze – odpowiednio – w katalogu swoich zadań otrzymały: udzielanie osobie, której dane dotyczą, na jej żądanie, informacji o wykonywaniu praw przysługujących im na mocy RODO, a w stosownym przypadku współpracowanie w tym celu z organami nadzorczymi innych państw członkowskich (art. 57 ust. 1 lit. e RODO). Zatem również w zakresie szerzenia wiedzy i udzielania pomocy występuje podobieństwo obowiązków organów nadzorczych i inspektorów ochrony danych, co prowadzi do wniosku, że również na tej płaszczyźnie działania tych podmiotów będą się uzupełniać.

W zakresie edukacji należy dostrzec jeszcze jedno pole integracji wysiłków GIODO i inspektorów ochrony danych – wzajemną wymianę informacji i doświadczeń w przypadku szczególnie problematycznych zagadnień. In-

formacje na temat takich zagadnień mogą być przekazywane inspektorom ochrony danych przez organ nadzorczy na podstawie sygnałów pochodzących m.in. od podmiotów danych czy organów nadzorczych w innych państwach członkowskich UE. Z drugiej strony – administratorzy bezpieczeństwa informacji dotychczas wielokrotnie identyfikowali, a następnie zgłasza- li GIODO najpoważniejsze problemy prawne i faktyczne pojawiające się w praktyce wykonywania ich funkcji. Dzięki temu możliwe jest wspólne szukanie rozwiązań zauważonych problemów, m.in. poprzez działania legislacyjne. Jednym z realizowanych obecnie (art. 12 pkt 5), jak i przyszłych⁷ zadań GIODO, jest bowiem opiniowanie projektów ustaw i rozporządzeń doty-

czących ochrony danych osobowych i w zakresie, w jakim projekty aktów prawnych dotyczyć będą działalności ABI – ich opinia z pewnością będzie dla GIODO bardzo istotna.

► Podstawa prawna

- art. 37–39, art. 57, art. 58, art. 83 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE Nr L 119 z 4.5.2016 r.)

⁶ Wynika to wprost z art. 12 ust. 2 zd. 1 oraz motywu 59 RODO.

⁷ Zgodnie z art. 57 ust. 1 lit. c oraz lit. i RODO, każdy organ nadzorczy na swoim terytorium doradza parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych, a także monitoruje zmiany w stosownych dziedzinach, w szczególności rozwój technologii informacyjno-komunikacyjnych i praktyk handlowych.

Podsumowanie

Niewątpliwie warunkiem każdej efektywnej współpracy, każdego dobrego partnerstwa, jest wzajemne rozumienie się i wspieranie. Dlatego ważne jest, aby zarówno organ ochrony danych, jak i inspektorzy ochrony danych w poczuciu odpowiedzialności za to partnerstwo dokładali starań, aby ich współpraca w osiąganiu zbieżnych celów była jak najbardziej harmonijna.