

Rodo a obowiązki informatyków i inspektorów

OCHRONA DANYCH OSOBOWYCH

Nowe rozporządzenie unijne porządkuje zadania stojące przed osobami odpowiedzialnymi za ochronę danych. Istotne jest tutaj rozróżnienie ról, jakie odgrywają administratorzy systemów informatycznych i inspektorzy ochrony danych.

Andrzej Kaczmarek

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (rodo) weszło w życie w dniu 25 maja 2016 r. Będzie miało zastosowanie od 25 maja 2018 r. Art. 37 rodo wprowadza instytucję Inspektora Ochrony Danych (IOD), którym może być osoba posiadająca kwalifikacje zawodowe w zakresie ochrony danych osobowych, a w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych (art. 37 ust. 5 rodo). Zadania, jakie rodo stawia przed IOD, są w niektórych obszarach bardzo podobne do zadań, jakie przypisane są administratorom bezpieczeństwa informacji (ABI) w obecnie obowiązującej ustawie o ochronie danych osobowych (patrz: **tabela „Porównanie zadań ABI oraz IOD”**).

Podział obowiązków wynikających z rodo

W porównaniu z obecnie obowiązującą dyrektywą 95/46/WE rodo stawia administratorom i podmiotom przetwarzającym wiele nowych zadań. Są to m.in. zadania w zakresie:

- realizacji prawa do „bycia zapomnianym” oraz prawa do przeniesienia danych,

Realizacją obowiązków wynikających z rodo w zakresie zapewnienia zgodności przetwarzania danych z określonymi tam warunkami obciążeni są formalnie administrator danych osobowych i podmiot przetwarzający.

- wymagań, jakie muszą być spełnione w przypadku, gdy skutkiem przetwarzania jest automatyczne podejmowanie decyzji, w tym profilowanie,
- obowiązku przeprowadzenia oceny skutków dla ochrony danych, jeśli rodzaj przetwarzania, w tym stosowana technologia, może powodować wysokie ryzyko naruszenia prywatności,
- obowiązku uwzględnienia ochrony danych w fazie projektowania,
- zapewnienia takiej konfiguracji systemów, która domyślnie zapewnia ochronę danych.

Kwestią otwartą jest jednak podjęcie decyzji dotyczącej tego, kto poszczególne zadania ma wykonywać, jak one powinny być wykonywane oraz kto ma weryfikować ich wykonywanie. Art. 39 ust. 1 rodo stanowi, że zadaniem IOD jest: „informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub

Obowiązek powołania Inspektora Ochrony Danych

Zgodnie z art. 37 rodo wyznaczenie Inspektora Ochrony Danych jest obowiązkowe, gdy:

- przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości,
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 rodo, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 rodo.

W pozostałych sytuacjach o wyznaczeniu IOD może zdecydować ADO, chyba że obowiązek jego wyznaczenia wynika z innych przepisów prawa Unii Europejskiej lub przepisów państwa członkowskiego.

państw członkowskich o ochronie danych i doradzanie im w tych sprawach” (art. 39 ust. 1 pkt a) oraz „monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty” (art. 39 ust. 1 pkt b).

W praktyce powyższe zadania IOD powinien realizować poprzez monitorowanie zdefiniowanych przez administratora danych lub podmiot przetwarzający operacji przetwarzania danych

Porównanie zadań ABI oraz IOD

| Lp. | Zadania ABI wynikające z ustawy o ochronie danych osobowych | Zadania IOD/ADO wynikające z rodo |
|-----|---|---|
| 1. | Art. 36a ust. 2 pkt 1 litera a Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych. | Art. 39 ust. 1 lit. a Monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu oraz powiązane z tym audyty. |
| 2. | Art. 36a ust. 2 pkt 1 litera a Zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych. | Art. 39 ust. 1 lit. a (ciąg dalszy) (...) działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. Art. 39 ust. 1 lit. b Informowanie ADO/Procesora oraz pracowników, którzy przetwarzają dane, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie. |
| 3. | Art. 19b ust. 1 i 2 1. Generalny Inspektor może zwrócić się do administratora bezpieczeństwa informacji wpisanego do rejestru, o którym mowa w art. 46c, o dokonanie sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia. 2. Po dokonaniu sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, administrator bezpieczeństwa informacji, za pośrednictwem administratora danych, przedstawia Generalnemu Inspektorowi sprawozdanie, o którym mowa w art. 36a ust. 2 pkt 1 lit. a. | Art. 39 ust. 1 lit. a (ciąg dalszy) (...) działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. Art. 39 ust. 1 lit. d Współpraca z organem nadzorczym. Art. 39 ust. 1 lit. f Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach. |
| 4. | Art. 36a ust. 2 pkt 2 Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7. | Art. 30 ust. 1 (zadanie ADO) Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. |
| 5. | Art. 36a ust. 2 pkt 1 litera b Nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych. | Art. 24 ust. 1, 2 i 3 (zadanie ADO) 1. (...) administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądowi i uaktualnianie. 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych. 3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków. |
| 6. | Art. 36a ust. 2 pkt 2 Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7. | Brak. |
| 7. | Brak. | Art. 39 ust. 1 lit. c; art. 35 ust. 7 Udzielanie na żądanie ADO zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35. |

→ oraz aktywny udział w ich modyfikacji lub ustanawianiu nowych. Udział ten w odniesieniu do modyfikacji lub ustanawiania nowych operacji przetwarzania nie powinien się ograniczać tylko do kontroli zgodności przedstawionych przez ADO lub informatyków propozycji z przepisami prawa – powinien obejmować także przedstawianie własnych propozycji. W szczególności w przypadku stwierdzenia, że zaproponowane przez ADO, informatyków lub inne osoby rozwiązania naruszają przepisy rodo, IOD powinien mieć możliwość władczego oddziaływania. Oddziaływanie to może odbywać się poprzez przedstawienie własnych sugestii rozwiązań lub wskazanie wad w zaproponowanym rozwiązaniu, które należy usunąć w celu minimalizacji ryzyka związanego z przetwarzaniem danych (patrz motyw 77 rodo). Zgodnie z powyższym należy przyjąć przedstawiony poniżej podział zadań.

Zadania administratora danych osobowych i podmiotów przetwarzających

Realizacją obowiązków wynikających z rodo w zakresie zapewnienia zgodności przetwarzania danych z określonymi tam warunkami obciążeni są formalnie administrator danych osobowych (ADO) i podmiot przetwarzający. Nie oznacza to jednak, że osoby pełniące funkcję ADO – takie jak np. burmistrz, wójt, dyrektor lub prezes – poszczególne zadania zobowiązane są wykonywać osobiście. Osoby te zobowiązane są jednak do takich działań organizacyjnych, aby poszczególne zadania wynikające z rodo przypisane zostały do odpowiednich osób i aby były właściwie realizowane. Należy się zatem spodziewać, że w większości podmiotów, tak jak jest to obecnie w wielu podmiotach, za bezpieczeństwo systemów informatycznych – w tym za zapewnienie ochrony przetwarzanych przy ich użyciu danych osobowych, czyli zapewnienie poufności, integralności i dostępności przetwarzanych danych – odpowiedzialni będą administratorzy systemów informatycznych. W dużych organizacjach – w zależności od liczby, rozproszenia i stopnia skomplikowania

systemów informatycznych – mogą to być wydzielone specjalnie do takich zadań zespoły działające w odrębnej komórce organizacyjnej. Zadaniem ADO, niezależnie od przypisania poszczególnych zadań odpowiednim osobom lub komórkom organizacyjnym, jest podejmowanie decyzji w kwestiach dotyczących chociażby ustanawiania jakości i skuteczności podejmowanych działań, w tym podejmowania decyzji o tym, czy w danych okolicznościach pozostające tzw. szcztątkowe ryzyko utraty poufności przetwarzanych danych jest akceptowalne pomimo zastosowanych środków bezpieczeństwa.

Zadania Inspektora Ochrony Danych

Zgodnie z art. 39 rodo do głównych zadań IOD należy:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Jak wynika z powyższego wykazu, IOD ma wspierać ADO w podejmowaniu decyzji dotyczących procesów przetwarzania danych osobowych oraz monitorowania poprawności ich wykonywania. Należy zaznaczyć, że osoba wyznaczona do pełnienia funkcji IOD powinna

Podział zadań w przypadku wielu administratorów danych

Polski ustawodawca w art. 23 ust. 2a ustawy o ochronie danych osobowych, która jest implementacją dyrektywy 95/46/WE, uznał podmioty publiczne za jednego administratora danych, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu. Niefortunny powstała w ten sposób instytucja współadministratora, co stoi w sprzeczności z treścią obecnie obowiązującego unijnego aktu prawnego, gdyż żadna z jej norm nie uprawnia krajowego ustawodawcy do takich praktyk. Należy więc nadal traktować administratorów danych jako odrębne podmioty, z tymi samymi prawami

i obowiązkami. Problem ten rozwiązuje rodo w artykule 26. Wspólnie ustalone cele i sposoby przetwarzania przez co najmniej dwóch administratorów sprawia, że stają się oni współadministratorami. Tak więc zobowiązani są oni do określenia w przejrzysty sposób odpowiednich zakresów swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z rodo, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przystępujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 rodo, chyba że przypadające im obowiązki i ich

zakres określa prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. Należy zaznaczyć, że uzgodnienia nie wyłączają możliwości wykonywania przez osobę, której dane dotyczą, prawa wynikającego z rodo wobec każdego z administratorów. W przypadku współadministracji wyraźnie muszą być określone również zadania poszczególnych administratorów w innych obszarach, a szczególnie podział obowiązków w zakresie zarządzania bezpieczeństwem przetwarzania, o którym mowa w sekcji 2 rodo dotyczącej bezpieczeństwa danych osobowych.

Wykaz informacji zawartych w rejestrze czynności przetwarzania

| Lp. | Zawartość rejestru czynności przetwarzania prowadzonego przez ADO | 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. | Brak. |
| 3. | Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych. | Kategorie przetwarzania 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. | Brak. |
| 5. | Gdy ma to zastosowanie, informacja o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi – dokumentacja odpowiednich zabezpieczeń. | Gdy ma to zastosowanie, informacja o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi – dokumentacja odpowiednich zabezpieczeń. |
| 6. | Jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych. | Brak. |
| 7. | Jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. | Jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. |

Przepisy rodo, podobnie do obecnie obowiązującej ustawy o ochronie danych osobowych, w szczególnych przypadkach wymagają prowadzenia rejestru czynności przetwarzania danych osobowych. Jego zawartość jest podobna do zawartości rejestru zbiorów danych osobowych, do prowadzenia którego zobowiązani są obecnie administratorzy bezpieczeństwa informacji.

mieć odpowiednie kwalifikacje zawodowe i wiedzę fachową z zakresu prawa i praktyk w dziedzinie ochrony danych osobowych. W szczególności powinna ona posiadać wiedzę oraz umiejętności umożliwiające jej właściwe wykonywanie zadań, o których mowa wyżej.

Spoczywające na IOD zadania to nie tylko ocena zgodności z przepisami prawa aktualnego stanu wdrożonych procedur przetwarzania danych, lecz także doradzanie w zakresie wdrażania nowych rozwiązań biznesowych. Jednym z istotnych elementów tych działań jest, jak wspomniano wyżej, udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rodo. Ocena skutków dla ochrony danych powinna być przeprowadzana zawsze wtedy, gdy występują elementy zautomatyzowanego przetwarzania danych, w tym profilowanie osób fizycznych, których skutki mogą znacząco wpływać na osobę fizyczną, lub gdy przetwarzaniu na dużą

skalę poddawane są szczególne kategorie danych osobowych (patrz: art. 9 ust. 1 oraz art. 10 rodo). Ocena skutków dla ochrony danych powinna być przeprowadzana także wtedy, gdy przetwarzanie polega na systematycznym monitorowaniu na dużą skalę miejsc dostępnych publicznie.

Przygotowanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania wymagać będzie od IOD głębokiej i wszechstronnej analizy przedstawianego projektu przetwarzania oraz przeprowadzenia oceny przewidzianych środków bezpieczeństwa. Innymi słowy, rodo nie nakłada na IOD wprost obowiązku wykonywania jakichkolwiek działań bezpośrednio

sprawczych, takich jak np. wykonywanie obowiązku informacyjnego wobec podmiotów danych, wykonanie oceny skutków dla ochrony, o których mowa w art. 35 rodo, czy też określenia środków, jakie powinny być wdrożone w ramach obowiązku uwzględnienia ochrony danych w fazie projektowania, oraz domyślnej ochrony danych. Do bezpośrednich zadań IOD nie należy również wdrażanie środków bezpieczeństwa ochrony danych, o których mowa w art. 32 rodo. Zadaniem IOD jest w powyższym zakresie ocena proponowanych lub zastosowanych już rozwiązań. Nie oznacza to jednak, że ADO nie może się zwrócić do IOD o przygotowanie wytycznych do realizacji wymienionych wyżej zadań, aby następnie ich wykonanie zlecić administratorowi systemu informatycznego (ASI). Podstawą do takich działań jest wspomniany już art. 39 ust. 1 pkt A rodo, który stanowi, że zadaniem IOD jest:

informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.

Należy w związku z powyższym przyjąć, że ostatecznie ADO lub podmiot przetwarzający decyduje o tym, komu i jakie zadania operacyjne wynikające z przepisów rodo należy powierzyć.

Obowiązki Administratora Systemu Informatycznego w zakresie ochrony danych osobowych

Rodo wskazuje w tym zakresie jedynie, że ADO i podmioty przetwarzające stosownie do okoliczności powinny wdrożyć odpowiednie środki zapewniające, w tym m.in. w stosownym przypadku: →

Rodo – w przeciwieństwie do obecnie obowiązującej ustawy o ochronie danych osobowych – nie wymaga od administratorów ani od podmiotów przetwarzających stosowania ściśle określonych środków bezpieczeństwa.


-
- 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.

Użyte przed powyższym wyliczeniem sformułowanie „w stosownym przypadku” pozostawia ADO w powyższym obszarze pełną swobodę. Pozostawiona swoboda ma uzasadnienie np. w odniesieniu do takich środków, jak pseudonimizacja i szyfrowanie, które muszą być zastosowane w szczególnych okolicznościach. Ogólnym wymaganiem w zakresie wdrożenia środków ochrony jest, aby wdrożone środki techniczne i organizacyjne zapewniały właściwy stopień bezpieczeństwa przetwarzanych danych, uwzględniając m.in.: 1) koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania; 2) ryzyko naruszenia ochrony danych z uwzględnieniem prawdopodobieństwa wystąpienia i wagi zagrożeń oraz 3) stan wiedzy technicznej. W praktyce oznacza to, że administratorzy oraz podmioty przetwarzające dane osobowe samodzielnie lub wspólnie z IOD muszą podjąć decyzje o tym, jakie techniczne i organizacyjne środki zastosować.

W wielu wypowiedziach dotyczących tej sprawy zwraca się uwagę na warunek, który mówi o tym, że zastosowane środki muszą uwzględniać stan wiedzy technicznej w tym zakresie. W rozporządzeniu nie mówi się o stanie wiedzy technicznej administratora danych, podmiotu przetwarzającego lub wyznaczonego IOD, co oznacza, że odniesieniem ma być ogólny stan wiedzy technicznej. Należy zatem przyjąć, że chodzi tutaj o wiedzę prezentowaną przede wszystkim w ogólnie przyjętych: normach dotyczących bezpieczeństwa systemów informatycznych, dobrych praktykach, kodeksach postępowania, przewodnikach, a także w wytycznych w tym



ADO zadaniami w zakresie zapewnienia bezpieczeństwa przetwarzania danych obciążać będą ASI. W rzeczywistości musi to być jednak wysiłek wspólny całego zespołu odpowiedzialnego za projektowanie, wdrażanie i utrzymywanie systemów informatycznych i sieci. Wysiłek ten musi oczywiście uwzględnić rzeczywistość, w jakiej działa administrator, czyli przede wszystkim warunki finansowe i biznesowe.

zakresie publikowanych przez producentów systemów informatycznych, producentów sprzętu informatycznego oraz architektów i projektantów systemów informatycznych. Należy zwrócić uwagę na fakt, że w większości przypadków będzie w tym zakresie wymagana wiedza specjalistyczna posiadana przez programistów, administratorów systemów informatycznych, administratorów sieci, specjalistów od zabezpieczeń oraz audytorów systemów informatycznych. W praktyce oznacza to, że ADO zadaniami w zakresie zapewnienia bezpieczeństwa przetwarzania danych obciążać będą ASI. W rzeczywistości musi to być jednak wysiłek wspólny całego zespołu odpowiedzialnego za projektowanie, wdrażanie i utrzymywanie systemów informatycznych i sieci. Wysiłek ten musi oczywiście uwzględnić rzeczywistość, w jakiej działa administrator, czyli przede wszystkim warunki finansowe i biznesowe. 

Autor jest dyrektorem Departamentu Informatyki w Biurze Generalnego Inspektora Ochrony Danych Osobowych.