Ius Novum
4/2016

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

RYSZARD SZAŁOWSKI

Na administratorze danych, zgodnie z treścią art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1] (dalej jako ustawa) ciąży obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien on zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych prowadzi dokumentację, w postaci polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym, opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Zakres i prowadzenie tej dokumentacji oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych określają przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.[2] Realizacja wspomnianych obowiązków wymaga opracowania i aktualizacji dokumentacji, wdrożenia przewidzianych w niej wymogów ochrony, właściwego przeszkolenia osób przetwarzających w jednostce organizacyjnej dane osobowe oraz zapewnienia kontroli przestrzegania przepisów ustawy, jak również rygorów wynikających z wdrożonej dokumentacji.

Dążąc do zapewnienia warunków realnej ochrony danych osobowych ustawodawca, nowelizując ustawę w 2004 r., dodał do treści art. 36 ustęp 3, zgodnie z którym administrator danych wyznacza administratora bezpieczeństwa informacji (dalej jako ABI), nadzorującego przestrzeganie zasad ochrony, chyba że sam wykonuje te czyn-

[1] Tekst jedn. Dz.U. z 2014 r. poz. 1182, ze zm.

[2] Dz.U. Nr 100, poz. 1024. W wyniku nowelizacji ustawy o ochronie danych osobowych dokonanej mocą postanowień art. 13 ustawy z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz.U. poz. 2281) obecnie zobowiązanym do wydania rozporządzenie regulującego wskazane w tekście zagadnienia jest minister właściwy do spraw informatyzacji.

ności[3]. Regulacja ta miała zatem charakter ramowy, nie przesądzała warunków, jakie ma spełnić osoba kandydująca do pełnienia tej funkcji, nie określała szczegółowo jej zadań, obowiązków ani uprawnień. Luka ta została uzupełniona postanowieniami jednej z kolejnych ustaw nowelizujących – ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (art. 9)[4], której postanowienia weszły w życie z dniem 1 stycznia 2015 r.[5]

Celem niniejszego artykułu jest prezentacja, analiza i ocena wdrożonych regulacji z punktu widzenia ich funkcji gwarancyjnej w odniesieniu do skuteczności ochrony danych osobowych.

1. POWOŁYWANIE I REJESTRACJA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Jak stanowi art. 36a ust. 1 ustawy, administrator danych może powołać administratora bezpieczeństwa informacji. Zatem, ustanowienie podmiotu bezpośrednio realizującego zadania w zakresie ochrony danych osobowych jest uprawnieniem, a nie obowiązkiem administratora. Skoro powołanie ABI jest fakultatywne to oznacza, że ustawodawca nie traktuje skuteczności ochrony danych osobowych jako okoliczności pierwszoplanowej, pozostawia administratorowi wybór, czy zadania bezpieczeństwa informacji powierzyć ABI, czy też przyjąć inną formę organizacyjną zapewnienia przestrzegania przepisów o ochronie danych osobowych[6]. Wzgląd na efektywność ochrony danych osobowych powinien, w moim przekonaniu, prowadzić do ustanowienia obowiązku powołania ABI przez administratora danych.

Z kolei przepis art. 36b stanowi, że w przypadku niepowołania ABI, jego zadania (z wyłączeniem wskazanych w tym przepisie) wykonuje administrator danych. Powołany wyżej przepis nie zobowiązuje administratora do osobistej realizacji takich obowiązków, zatem należy przyjąć że ustawodawca nie obligując administratora do powołania ABI zobowiązuje go do przyjęcia innej formy organizacyjnej działań, ukierunkowanych na skuteczność ochrony danych osobowych. M. Byczkowski wskazuje, że administrator danych może wyznaczyć do wykonywania takich zadań inne osoby, może także powierzyć ich realizację przedsiębiorcy w ramach outsourcingu[7]. Zatem,

---

[3] Art. 1 pkt 20 ustawy z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz.U. Nr 33, poz. 285).

[4] Dz.U. poz. 1662.

[5] Genezę instytucji ABI w ujęciu ewolucyjnym z uwzględnieniem analizy projektu wskazanej w tekście nowelizacji omawia P. Fajgielski, *Administrator bezpieczeństwa informacji – geneza, stan obecny i perspektywy zmian*, „Monitor Prawniczy" dodatek do nr 9/2014, s. 39–44.

[6] A. Mednis podkreśla, że „nic nie stoi na przeszkodzie, aby zamiast abi powołać do życia inne stanowisko lub funkcję związaną z ochroną danych osobowych" – zob. A. Mednis, *Administrator bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych z 7.11.2014 r. – ocena rozwiązań*, „Monitor Prawniczy" dodatek do nr 6/2015, s. 23.

[7] M. Byczkowski, *Zapewnianie przestrzegania przepisów o ochronie danych osobowych w sferze wewnętrznej bez powołania administratora bezpieczeństwa informacji*, „Monitor Prawniczy" dodatek do nr 6/2015, s. 8.

administrator może powierzyć wykonywanie zadań analogicznych do przypisanych ABI osobie, której nie powoła do pełnienia obowiązków ABI w rozumieniu ustawy.

Zdaniem P. Fajgielskiego, wyznaczenie ABI leży w interesie administratora „gdyż w ten sposób może zrzucić z siebie ciężar niektórych obowiązków (…) i związaną z tym odpowiedzialność”[8]. Jednak biorąc pod uwagę, że zgodnie z treścią art. 36 ust. 1 ustawy administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, należy uznać, że powołanie ABI nie zwalnia administratora danych od odpowiedzialności za uchybienia, jakie ewentualnie wystąpią w tym zakresie.

W ramach obowiązującej regulacji prawnej nie wskazano formy zatrudnienia osoby realizującej zadania ABI, podkreślono natomiast, że podmiot ten podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. Pozycję organizacyjną ABI wyznacza także ciążący na administratorze obowiązek zapewnienia środków i organizacyjnej odrębności ABI, niezbędnych do niezależnego wykonywania przez niego zadań. Bezpośrednia podległość administratorowi, organizacyjna odrębność oraz dysponowanie środkami realizacji powierzonych zadań mają stanowić gwarancje niezależności ABI od podmiotów przetwarzających dane osobowe, których zachowania, pod kątem zgodności z przepisami ustawy, są przedmiotem sprawdzeń prowadzonych przez ABI. „Bezpośrednia podległość kierownikowi jednostki ma stanowić jedną z gwarancji niezależności ABI względem innych osób w danej jednostce organizacyjnej”[9]. W doktrynie wskazuje się również, że „bezpośrednia podległość administratorowi danych ma umożliwiać skuteczne wykonywanie nadzoru nad przestrzeganiem przepisów o ochronie danych osobowych”[10].

Administrator danych może powierzyć ABI wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, a „ocena w tym zakresie powinna być dokonywana w konkretnym przypadku z uwzględnieniem wszystkich istotnych okoliczności faktycznych”[11]. Zdaniem A. Mednisa mogą to być zadania niezwiązane z ochroną danych osobowych i w ramach ich wykonywania ABI nie musi podlegać kierownikowi jednostki”[12].

W treści przepisu art. 36a ust. 5 określone zostały wymogi jakie ma spełniać osoba, która może zostać ABI. Zaliczono do nich: pełną zdolność do czynności prawnych, korzystanie z pełni praw publicznych, niekaralność za umyślne przestępstwo oraz posiadanie odpowiedniej wiedzy w zakresie ochrony danych osobowych.

Kontrowersyjnym jest umożliwienie powołania jako ABI osoby skazanej za przestępstwo nieumyślne. Okazanie karalnej lekkomyślności bądź niedbalstwa nie jest bowiem, w moim przekonaniu, okolicznością obojętną z punktu widzenia wiarygodności osoby skazanej jako podmiotu, któremu powierza się zapewnienie przestrzegania

---

[8] P. Fajgielski, *Pozycja prawna i zadania administratora bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych*, „Monitor Prawniczy” dodatek do nr 6/2015, s. 3.

[9] *Ibidem*, s. 4.

[10] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, wyd. VI – Lex, art. 36a teza 11.

[11] *Ibidem*, teza 9 do art. 36a.

[12] A. Mednis, *op. cit.*, s. 21.

przepisów o ochronie danych osobowych. Nawet skazanie za nieumyślne przestępstwo przeciwko ochronie danych osobowych nie dyskwalifikuje, w ramach obowiązujących przepisów, do pełnienia obowiązków ABI.

Ustawodawca nie określa poziomu ani profilu wykształcenia wymaganego od kandydata na ABI, natomiast stanowi, że posiadana przez niego wiedza w zakresie ochrony danych osobowych ma być odpowiednia, nie wskazując na formy jej weryfikacji. Poziom wiadomości ocenia administrator, jako podmiot powołujący ABI, jednak brak formalnych i faktycznych gwarancji, że sam administrator taką wiedzę posiada i jest w stanie zweryfikować adekwatność skuteczności edukacji kandydata, jeżeli posiadana przez niego wiedza nie jest potwierdzona dokumentami poświadczającymi co najmniej udział w stosownych szkoleniach. Określając merytoryczne wymagania stawiane kandydatowi na ABI, ustawodawca posłużył się zatem kryterium, które można ocenić jako subiektywne i minimalne, co trudno uznać za przejaw troski o zapewnienie skuteczności ochrony danych osobowych.

Na podstawie art. 46b ust. 1 ustawy administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi Ochrony danych Osobowych (dalej jako GIODO) powołanie ABI w terminie 30 dni. Jak zaznacza G. Sibiga „podstawowym celem rejestracji ABI jest zachowanie kontroli GIODO nad powoływaniem ABI oraz późniejszym wykonywaniem przez niego zadań”[13].

Istotnym błędem ustawodawcy jest zaniechanie wskazania skutków prawnych powołania do pełnienia funkcji ABI osoby, która nie spełnia wskazanych w ustawie warunków oraz niezgłoszenia powołania ABI do GIODO.

Jeżeli dojdzie do powołania do pełnienia funkcji ABI osoby niespełniającej ustawowych wymogów, to akt taki zachowuje ważność, albowiem ustawodawca nie przewidział procedury jego kontroli, nie wskazał podmiotu upoważnionego do jego uchylenia.

Wprawdzie zgłoszenie ABI do rejestracji stanowi obowiązek administratora danych, ale niezgłoszenie nie pozbawia tego podmiotu statusu administratora bezpieczeństwa informacji, a jedynie ogranicza zakres jego funkcji. Zgodnie z treścią art. 19b ustawy, GIODO może zwrócić się o dokonanie sprawdzenia u administratora jedynie do ABI wpisanego do rejestru. Z kolei według brzmienia przepisu art. 36b ustawy administrator danych wykonuje zadania ABI wskazane w art. 36a ust. 2 pkt 1 lit. a[14] w przypadku niepowołania ABI. Wynika stąd, że na administratorze, który powołał ABI, ale nie zgłosił tego faktu do rejestracji GIODO, nie ciążą wskazane wyżej obowiązki. Zatem to niezgłoszony do rejestracji ABI, a nie administrator danych będzie zobowiązany do zapewnienia przestrzegania przepisów o ochronie danych osobowych. Nadto z treści art. 43 ust. 1a ustawy wynika, że obowiązkowi rejestracji zbiorów danych osobowych nie podlega administrator danych, który powołał ABI i zgłosił go GIODO do rejestracji, a zatem ustawodawca odróżnia status ABI powołanego, a niezgłoszonego do rejestracji oraz ABI powołanego i zgłoszonego do rejestracji.

Wobec powyższego należy przyjąć, że ABI uzyskuje taki status z chwilą powołania i może realizować uprawnienia i obowiązki, z wyjątkiem wyłączonych przez ustawę

---

[13] G. Sibiga, *Rejestracja administratorów bezpieczeństwa informacji. Postępowanie rejestracyjne Generalnego Inspektora Ochrony Danych Osobowych*, „Monitor Prawniczy” dodatek do nr 6/2015, s. 13.

[14] O zakresie zadań ABI piszę w dalszych częściach artykułu.

z racji niewystąpienia o jego rejestrację, bądź niewpisania do rejestru. Jednocześnie warto zauważyć, że w ustawie nie przewidziano procedury egzekwowania od administratora realizacji obowiązku zgłoszenia ABI do rejestracji. Nie podzielam poglądu G. Sibigi, według którego GIODO jest upoważniony w stosunku do administratora danych, który nie zgłosił ABI do rejestracji, tak jak w przypadku innych stwierdzonych naruszeń przepisów o ochronie danych osobowych, do wydania na podstawie art. 18 ustawy „nakazu przywrócenia stanu zgodnego z prawem, w tym przypadku polegający na nakazaniu administratorowi danych zgłoszenia powołania ABI”[15]. Po pierwsze, z treści przesłanek takiej decyzji GIODO wskazanych w art. 18 ust. 1 pkt 1–6[16] (mimo otwartego charakteru tego wykazu) wynika, że wydane nakazy mają odnosić się do czynności bezpośrednio związanych z ochroną danych osobowych przetwarzanych u administratora. Po drugie, należy podkreślić, że nawet niepowołanie ABI nie stanowi naruszenia prawa przez administratora albowiem jest to jego uprawnienie, a nie obowiązek. Wreszcie, po trzecie, jak starałem się wyżej wykazać, ustawodawca odróżnia status ABI powołanego i zgłoszonego do rejestracji oraz ABI, który został powołany, ale nie zgłoszono go do rejestracji. Zatem, stan powołania ABI i niezgłoszenia go do rejestracji został przez ustawodawcę przewidziany.

Zgłoszenie powołania ABI do rejestracji powinno zawierać:

– oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;
– dane ABI, takie jak:
  a) imię i nazwisko;
  b) numer PESEL lub, gdy ten numer nie został nadany, nazwę i numer dokumentu stwierdzającego tożsamość;
  c) adres do korespondencji, jeżeli jest inny niż adres siedziby lub miejsca zamieszkania administratora;
  d) datę powołania;
  e) oświadczenie administratora danych o spełnianiu przez ABI warunków umożliwiających powołanie oraz świadczących o bezpośredniej podległości kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.

Wzór zgłoszenia powołania ABI do rejestracji GIODO został ustalony treścią załącznika nr 1 do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r.[17] W częściach A i B zgłoszenia zawarto szczegółowe informacje służące identy-

---

[15] G. Sibiga, *op. cit.*, s. 14.

[16] Należą do nich:
1) usunięcie uchybień;
2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych;
3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;
4) wstrzymanie przekazywania danych osobowych do państwa trzeciego;
5) zabezpieczenie danych lub przekazanie ich innym podmiotom;
6) usunięcie danych osobowych.

[17] Rozporządzenie w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. poz. 1934).

fikacji administratora oraz ABI, a część C stanowi oświadczenie administratora danych o spełnieniu przez ABI warunków określonych w ustawie. G. Sibiga trafnie zauważa, że w oświadczeniu tym pominięto warunek „zapewnienia środków i organizacyjnej odrębności ABI niezbędnych do niezależnego wykonywania zadań”[18].

Wpisanie ABI do rejestru następuje w formie czynności materialno-technicznej. Ustawodawca nie przewidział możliwości odmowy dokonania takiej czynności. Jednak rejestracja może nastąpić tylko w sytuacji, kiedy zgłoszenie zawiera w poprawnej formie wszystkie wymagane informacje. Ich brak stanowi, w moim przekonaniu podstawę do wezwania administratora w trybie art. 64 § 2 Kodeksu postępowania administracyjnego[19] do usunięcia braków w terminie siedmiu dni z pouczeniem, że nieusunięcie tych braków spowoduje pozostawienie podania bez rozpoznania[20].

Bardziej złożoną jest sytuacja, gdy zgłoszenie powołania ABI do rejestracji zawiera wszystkie wymagane informacje, ale z ich treści wynika, że osoba powołana do pełnienia funkcji ABI nie spełnia wymagań określonych w ustawie. Brak przepisu upoważniającego GIODO do odmowy rejestracji ABI. Według stanowiska G. Sibigi „GIODO nie może postąpić inaczej niż odmawiając wpisu rejestracyjnego, gdy stwierdzi, że zgłoszony ABI nie spełnia rygorów kwalifikacyjnych”[21]. W ramach przedstawionej argumentacji cytowany Autor podkreśla, iż według stanowiska orzecznictwa sądowego odmowa wykonania czynności materialno-technicznej następuje w formie decyzji administracyjnej, nawet jeśli nie przewidują tego wprost przepisy ustawy. Odmowa wpisu ABI do rejestru nie pozbawia tego podmiotu, jak sądzę, możliwości wykonywania przewidzianych w ustawie zadań (z wyjątkiem kompetencji przysługujących ABI zarejestrowanemu).

Na żądanie administratora danych lub ABI – GIODO wydaje zaświadczenie o zarejestrowaniu ABI.

GIODO prowadzi ogólnokrajowy, jawny[22] rejestr administratorów bezpieczeństwa informacji, zawierający:

– informacje o administratorze danych i adresie jego siedziby lub miejscu zamieszkania, w tym numerze identyfikacyjnym rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;
– dane ABI, takie jak: imię i nazwisko oraz adres do korespondencji, jeżeli jest inny niż adres siedziby lub miejsca zamieszkania administratora[23].

---

[18] G. Sibiga, *op. cit.*, s. 14.

[19] Tekst jedn. Dz.U. z 2016 r. poz. 23.

[20] Podobne stanowisko prezentuje G. Sibiga, *op. cit.*, s. 18.

[21] G. Sibiga, *op. cit.*, s. 17.

[22] A. Mednis ocenia jawność rejestru jako posunięcie zbyt daleko idące, które może zniechęcić administratorów danych do powoływania ABI – zob. A. Mednis, *op. cit.*, s. 23.

[23] J. Barta i in. słusznie stwierdzają, że „wątpliwości budzi brak wskazania w rejestrze daty powołania ABI”. Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, art. 46c, teza 2. Także G. Sibiga wskazuje na brak w rejestrze abi prowadzonym przez GIODO informacji o dacie powołania ABI, co ma to istotne znaczenie albowiem „od tego dnia abi jest zobligowany do prowadzenia jawnego, wewnętrznego rejestru zbiorów. Zob. *op. cit.*, s. 16. Z kolei J. Fajgielski przytacza argumenty przeciwko obowiązkowi rejestracji ABI, wskazując na dodatkowe obciążenie administratora, co może przemawiać przeciwko powoływaniu ABI i postulując poprzestanie na zobowiązaniu administratora danych do zapewnienia jawności informacji o powołaniu ABI. Zob. *Administrator…*, s. 43.

Administrator danych jest obowiązany zgłosić GIODO zmianę informacji objętych zgłoszeniem w terminie 14 dni od dnia zmiany. Zgłoszeniu do GIODO podlega również odwołanie ABI. Obowiązek ten administrator powinien zrealizować w terminie 30 dni od odwołania. Regulacja taka budzi wątpliwości, albowiem termin na poinformowanie o zmianach informacji objętych zgłoszeniem jest krótszy niż termin zgłoszenia odwołania, które wywołuje przecież dalej idące skutki prawne.

Zgłoszenie odwołania ABI powinno zawierać: imię i nazwisko ABI, numer PESEL oraz datę i przyczynę odwołania. Wzór zgłoszenia odwołania ABI został określony w załączniku nr 2 do wskazanego ostatnio rozporządzenia.

Zgodnie z treścią art. 46d ustawy powiadomienie GIODO przez administratora o odwołaniu ABI skutkuje wykreśleniem tego podmiotu z rejestru. GIODO wykreśla ABI z rejestru także w przypadku jego śmierci, jednak ustawodawca wprost nie nakłada na administratora obowiązku powiadomienia GIODO o takim zdarzeniu.

Wykreślenie ABI z rejestru może również nastąpić z urzędu. GIODO wydaje w tym przedmiocie decyzję administracyjną, gdy ABI:
– utracił pełną zdolność do czynności prawnych, przestał spełniać warunek niekaralności za przestępstwo umyślne, został pozbawiony praw publicznych;
– nie spełnia warunku posiadania odpowiedniej wiedzy w zakresie ochrony danych osobowych;
– nie podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych, bądź
– nie wykonuje zadań określonych w ustawie[24].

Należy postawić pytanie, czy w ramach przesłanki wskazanej jako ostatnia chodzi o niewłaściwe, niestaranne, merytorycznie niepoprawne wykonywanie zadań przez ABI, czy też o sytuację odsunięcia ABI od wykonywania zadań ustawowych i powierzenia mu innych obowiązków. Sądzę, że ponieważ w treści przepisu (art. 46d ust. 2 pkt 2) zabrakło wskazania na przesłanki wartościujące (*verba legis*: nie wykonuje zadań) właściwą jest druga ze wskazanych interpretacji[25].

Wykreślenie ABI z rejestru następuje z urzędu również wówczas, gdy administrator danych nie powiadomił GIODO o jego odwołaniu. W takiej sytuacji nie jest istotne źródło, z którego GIODO uzyskał informacje o okolicznościach mających stanowić podstawę wykreślenia ABI z rejestru. Decyzja o wykreśleniu ma charakter związany (*verba legis*: wydaje decyzję o wykreśleniu). Należy jednak odpowiedzieć na pytanie o status ABI wykreślonego z rejestru. W mim przekonaniu nadal jest on upoważniony do wykonywania zadań, z ograniczeniami wynikającymi z ustawy, a dotyczącymi ABI niezarejestrowanego, chyba że wykreślenie z rejestru nastąpiło w wyniku jego śmierci. Nie podzielam stanowiska G. Sibigi, że jednocześnie z wykreśleniem GIODO „winien (…) wydać decyzję nakazującą administratorowi przywrócenie stanu zgodnego

[24] A. Mednis trafnie spostrzega, że wśród wymienionych przesłanek nie wskazano na brak dysponowania przez ABI środkami realizacji powierzonych zadań i organizacyjnej odrębności tego podmiotu. Zob. A. Mednis, *op. cit.*, s. 20.

[25] W doktrynie przedstawiono również stanowisko, zgodnie z którym wydanie przez GIODO decyzji o wykreśleniu ABI z rejestru administratorów bezpieczeństwa informacji może być „konsekwencją nieprzeprowadzenia przez ABI sprawdzenia bądź nieprzedstawienia GIODO sprawozdania". Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, art. 19b teza 5.

z prawem (na podstawie art. 18 ust. 1 ustawy)”[26]. Przedmiotem decyzji GIODO jest wykreślenie ABI z rejestru, należy zatem przyjąć, że gdyby wolą ustawodawcy było uchylenie skutków prawnych powołania ABI, to wskazałby na zaistnienie ich z mocy prawa. Przepis art. 18 ust. 1 ustawy, jak argumentowałem to wcześniej, nie może stanowić podstawy do wydawania przez GIODO decyzji innych, niż odnoszących się bezpośrednio do przetwarzania danych u administratora. Ustawodawca nie przewidział mechanizmów kontroli prawidłowości powoływania ABI przez administratora danych, ustalił jedynie przesłanki zarejestrowania ABI przez GIODO, przyzwalając jednocześnie na funkcjonowanie ABI niezgłoszonego do rejestracji i być może niespełniającego ustawowych warunków powołania. Taki stan prawny nie zasługuje na akceptację, jednak jego zmiana może nastąpić jedynie w rezultacie stosownej nowelizacji ustawy.

Jeżeli ABI pełni taką funkcję u więcej niż jednego administratora, wówczas zaistnienie przesłanki utraty pełnej zdolności do czynności prawnych, skazanie za przestępstwo umyślne, bądź stwierdzenie braku posiadania przez ABI odpowiedniej wiedzy w zakresie ochrony danych osobowych dyskwalifikuje taką osobę „do pełnienia funkcji ABI u jakiegokolwiek administratora danych, a zatem konsekwentnie decyzja GIODO o wykreśleniu ABI powinna być w takich przypadkach kierowana do wszystkich podmiotów, u których pełni on taką funkcję”[27].

Ustawodawca przewidział również (art. 46e ustawy) możliwość ponownego zgłoszenia przez administratora danych do rejestracji przez GIODO powołania ABI wykreślonego uprzednio z rejestru. W takiej sytuacji GIODO wpisuje ABI do rejestru po stwierdzeniu, że nie zachodzą przyczyny wykreślenia, z wyjątkiem sytuacji, gdy podstawę wykreślenia stanowiło niepowiadomienie GIODO przez administratora o odwołaniu ABI. W tej ostatnio wskazanej sytuacji ponowne powołanie tej samej osoby do pełnienia funkcji ABI będzie stanowiło podstawę zgłoszenia do rejestracji na ogólnych zasadach. Z kolei, GIODO odmawia wpisania ABI do rejestru, jeżeli nie zostały usunięte przyczyny wykreślenia z rejestru. W tym kontekście należy podkreślić, że do dokonania wpisu nie wystarczy usunięcie przyczyn wykreślenia. Odmowa powinna nastąpić także wówczas, jeżeli mimo ich usunięcia zaistniały inne przesłanki negatywne świadczące o tym, iż ABI, (także jego organizacyjne posadowienie) nie spełnia w sposób wyczerpujący wymogów ustawowych.

Art. 36a ust. 6 ustawy umożliwia powołanie przez administratora danych zastępców ABI. Powinni oni spełniać warunki stawiane kandydatowi na ABI. Ponieważ ustawodawca nie upoważnia ABI do ustalenia zadań zastępców wynika stąd, że zadania te określa podmiot powołujący, czyli administrator danych. Zastępcy ABI nie podlegają wpisowi do rejestru prowadzonego przez GIODO. Nie podzielam prezentowanego w doktrynie stanowiska, że stworzenie przez ustawodawcę możliwości powołania ABI nie oznacza zakazu powołania więcej niż jednego ABI[28]. Sądzę, że wprowadzenie instytucji zastępcy ABI czyni procedurę powołania więcej niż jednego ABI bezprzedmiotową.

Reasumując uwagi odnoszące się do prawnych podstaw powoływania i rejestracji ABI postuluję ustanowienie skuteczności powołania ABI przez administratora dopiero

---

[26] G. Sibiga, *op. cit.*, s. 18.
[27] A. Mednis., *op. cit.*, s. 23.
[28] P. Fajgielski, *Pozycja prawna…*, *op. cit.*, s. 5.

po jego rejestracji przez GIODO, przyjęcie, że odmowa rejestracji następuje w formie decyzji administracyjnej, a wykreślenie ABI z rejestru pozbawia go uprawnień do realizacji zadań wskazanych w ustawie.

2. ZAPEWNIANIE PRZESTRZEGANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH JAKO ZADANIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Pierwszym z zadań jakie przepisy ustawy wyznaczają ABI jest zapewnianie przestrzegania przepisów o ochronie danych osobowych (art. 36 ust. 2 pkt 1). Zadanie takie powinno być realizowane w szczególności przez:

– sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych;
– nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
– zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Ustawodawca nie odnosi się wprost do zakresu podmiotowego wskazanych wyżej czynności ABI co, w moim przekonaniu, oznacza że będą nimi objęte wszystkie podmioty zobowiązane do przestrzegania przepisów o ochronie danych osobowych oraz opracowania i aktualizowania dokumentacji, a pośrednio także administrator danych, jako odpowiedzialny za ochronę danych.

Tryb i sposób realizacji wspomnianych zadań zostały określone w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r.[29]

W pierwszej kolejności rozporządzenie określa tryb i sposób sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania w tym zakresie. Należy uznać, że chodzi tu nie tylko o przepisy ustawy o ochronie danych osobowych, ale również inne regulacje dotyczące tego tematu.

Jako sprawdzenie określono czynności ABI mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami. Może ono być wykonywane dla administratora danych, bądź dla GIODO. Sprawdzenie może mieć charakter planowany bądź doraźny.

W szczególności należy uwzględnić w planie sprawdzeń zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych z odpowiednimi przepisami ustawy. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabez-

[29] Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. poz. 745).

pieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat. Wskazaną w rozporządzeniu częstotliwość weryfikacji należy uznać, w moim przekonaniu, za zdecydowanie niewystarczającą. Nie stwarza ona podstawy właściwego zabezpieczenia interesów osób, których dotyczą dane. Plan sprawdzeń jest przygotowywany przez ABI na okres nie krótszy niż kwartał i nie dłuższy niż rok. Dokument taki podlega przedstawieniu administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.

Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu przez ABI wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

Na podstawie art. 19b. ust 1 ustawy GIODO może zwrócić się do ABI wpisanego do rejestru o dokonanie sprawdzenia u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia. W takim przypadku dokonanie sprawdzenia przez ABI nie wyłącza prawa GIODO do przeprowadzenia kontroli[30].

ABI zawiadamia administratora danych o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia realizowanego na zlecenie GIODO przed podjęciem pierwszej czynności. Nadto zawiadomienie powinno zostać skierowane, w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności, do kierownika jednostki organizacyjnej objętej sprawdzeniem, a przedmiotem zawiadomienia powinien być zakres planowanych czynności. Zawiadomienia nie przekazuje się w przypadku:

– sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce;
– sprawdzenia, o którego dokonanie zwrócił się GIODO, jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin oraz
– jeżeli kierownik jednostki organizacyjnej objętej sprawdzeniem posiada informacje o zakresie planowanych czynności.

Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze w nim udział lub umożliwia ABI przeprowadzenie czynności w toku sprawdzenia. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych, czynności ABI mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych, w szczególności osoby zarządzającej tym systemem.

ABI dokumentuje[31] czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie takich danych oraz do opracowania sprawozdania.

Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie w postaci elektronicznej albo papierowej, które przekazuje administratorowi danych (w terminie 30 dni

---

[30] Na temat kompetencji ABI w stosunkach z GIODO w okresie przed 1 stycznia 2015 r. zob. B. Pilc, *Rola administratora bezpieczeństwa informacji podczas inspekcji prowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych*, „Monitor Prawniczy" dodatek do nr 7 z 2012 r., s. 37–42. Odnosząc się do obecnej regulacji A. Mednis ocenia, że w ten sposób ABI jest „kimś w rodzaju pośrednika pomiędzy administratorem danych a GIODO" – zob. *op. cit*., s. 22.

[31] Dokumentowanie czynności w toku sprawdzenia może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:

od zakończenia sprawdzenia planowego, a niezwłocznie po zakończeniu sprawdzenia doraźnego). Termin przekazania sprawozdania ze sprawdzenia, o którego przeprowadzenie zwrócił się GIODO określa ten organ. Rodzaje informacji wymaganych w treści sprawozdania określono szczegółowo w ustawie (art. 36c)[32].

Na tle zaprezentowanej wyżej prawnej regulacji zapewniania przestrzegania przepisów o ochronie danych osobowych, jako zadania ABI należy postawić kilka pytań.

Po pierwsze, ustawodawca redagując przedmiot omawianego zadania posługuje się określeniem sprawdzanie, nie używa terminu kontrola[33]. Jednak ten zabieg językowy nie zmienia faktu, że mamy tu do czynienia z kompetencjami kontrolnymi. Wskazany został przedmiot kontroli, wzorzec w postaci ustawowego opisu pożądanego stanu, legalność jako kryterium sprawdzania, a sprawozdanie ma obejmować m.in. opis stanu faktycznego oraz stwierdzone w tym kontekście przypadki naruszenia przepisów o ochronie danych osobowych. Zatem należy uznać, że wymagane przez ustawodawcę działania ABI spełniają warunki uznania ich za czynności kontrolne[34]. Warto dodać, że przepisy ustawy oraz rozporządzenia wykonawczego nie upoważniają ABI do stosowania w związku ze stwierdzonymi ewentualnie niedociągnięciami żadnych środków o charakterze władczym. Sprawdzanie jest dokonywane dla administratora danych, bądź

– sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
– odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
– sporządzeniu kopii otrzymanego dokumentu;
– sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
– sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

[32] Sprawozdanie powinno zawierać:
– oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania;
– imię i nazwisko ABI;
– wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
– datę rozpoczęcia i zakończenia sprawdzenia;
– określenie przedmiotu i zakresu sprawdzenia;
– opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
– stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
– wyszczególnienie załączników stanowiących składową część sprawozdania;
– podpis ABI, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy ABI na każdej stronie sprawozdania;
10) datę i miejsce podpisania sprawozdania przez ABI.

[33] P. Fajgielski już na etapie prac na projektem ustawy słusznie uznał określenie „sprawdzanie" za nieprecyzyjne i postulował użycie terminu „kontrola". Zob. *Administrator*…, s. 42.

[34] Barta i in. z jednej strony uznają celowość użycia w odniesieniu do zadań abi określenia „sprawdzanie„ co ma odróżniać je od kompetencji kontrolnych inspektorów Biura GIODO, jednak ostatecznie przyznają, że „porównanie tych zakresów może prowadzić do wniosku o daleko idących podobieństwach między tymi konstrukcjami prawnymi". Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit*., art. 36a, teza 6.

dla GIODO i to adresaci sprawozdań są uprawnieni do zlecenia działań o charakterze korekcyjnym.

Po drugie, sprawdzanie realizowane na zlecenie GIODO odbywa się, zgodnie ze sformułowaniem użytym w treści art. 19b ust. 1 ustawy „u administratora danych", co w moim przekonaniu oznacza, że przedmiotem sprawdzeń może być również – pośrednio – przestrzeganie przepisów o ochronie danych osobowych przez administratora. Za stanowiskiem takim przemawia fakt, że GIODO zwraca się o dokonanie sprawdzenia – według redakcji wskazanego wyżej przepisu – „do administratora bezpieczeństwa informacji", a nie do administratora danych. Argumentację taką umacnia okoliczność, że w zgłoszeniu rejestracyjnym podaje się adres do korespondencji ABI, jeżeli jest inny niż adres, siedziby lub miejsca zamieszkania administratora[35]. Taka regulacja może mieć istotne znaczenie w razie potrzeby sprawdzenia stanu faktycznego, w przypadku wpłynięcia do GIODO skargi pochodzącej od osoby której dane dotyczą, której przedmiotem byłyby działania bądź zaniechania administratora danych naruszające przepisy o ochronie danych osobowych.

P. Fajgielski wskazuje, że przedstawianie sprawozdania GIODO może stawiać ABI „w trudnej sytuacji wobec administratora danych (…) a niekiedy prowadzić do swoistego samooskarżenia"[36]. W odniesieniu do użytego ostatnio argumentu, nietrudno zauważyć, że posadowienie ABI w roli podmiotu sprawującego kontrolę wewnętrzną i uczestniczącego w kontroli zewnętrznej może nie stanowić wystarczającej gwarancji jego obiektywizmu. W innej z prac, cytowany wyżej autor postuluje ograniczenie uprawnień GIODO w zakresie jego relacji z ABI do uprawnienia żądania od administratora danych kopii sprawozdania sporządzonego przez ABI, albowiem w obecnej sytuacji ABI może być postrzegany jak „długie ramię GIODO" co może prowadzić do niepowoływania ABI[37].

Po trzecie, należy odnieść się do kwestii prawnego znaczenia wyników sprawdzania dokonywanego dla GIODO. W tym miejscu chciałbym przypomnieć, że dokonanie przez ABI sprawdzenia nie wyłącza prawa GIODO do przeprowadzenia kontroli, o której mowa w art. 12 pkt 1 ustawy. Zatem, ustalenia poczynione przez ABI działającego na zlecenie GIODO nie mogą, jak sądzę, stanowić podstawy wydawania decyzji administracyjnych przez ten organ. Tego rodzaju kompetencje GIODO winny znajdywać oparcie w ustaleniach dokonywanych przez kontrolerów działających w trybie przepisów art. 14–17 ustawy. Wyniki sprawdzeń dokonywanych przez ABI mogą co najwyżej inspirować potrzebę podjęcia kontroli, która będzie realizowana przez inspektorów Biura GIODO.

Po czwarte, przepisy rozporządzenia nakazują uwzględnienie w planie sprawdzeń m.in. konieczności weryfikacji zgodności przetwarzania danych osobowych przepisami art. 32–35 ustawy określającymi uprawnienia osoby, której dotyczą dane. Należy zauważyć, że wspomnianym uprawnieniom odpowiadają obowiązki administratora danych, a więc zadania ABI będą aktualizować się wyłącznie w sytuacji, gdy osoba ta skorzysta

---

[35] Taką praktykę J. Barta i in. uznają za niewłaściwą, prezentując stanowisko, według którego korespondencja kierowana przez GIODO do ABI „powinna być wysyłana na adres administratora danych". Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, art. 46b, teza 4. Również A. Mednis odnosi się krytycznie do wprowadzania do rejestru ABI adresu do korespondencji – zob. *op. cit.*, s. 23.

[36] P. Fajgielski, *Administrator…*, s. 43.

[37] P. Fajgielski, *Pozycja prawna…*, s. 6.

z przysługującego jej prawa kontroli przetwarzanych danych w formach przewidzianych w ustawie, a administrator zleci ABI przeprowadzenie stosownych sprawdzeń. Z kolei, ponieważ ustawodawca traktuje jako podmiot uprawniony osobę, której dotyczą dane, a jako podmiot zobowiązany administratora danych, to należy uznać, że ABI nie jest uprawniony do podejmowania rozstrzygnięć w kwestiach takich jak np. usunięcie ze zbioru danych zbędnych dla realizacji celu dla którego zostały zebrane, zasadności żądania zaprzestania przetwarzania danych ze względu na szczególną sytuację osoby, której dane dotyczą, czy wniesienia sprzeciwu wobec przetwarzania jej danych.

Rozporządzenie określa również tryb i sposób sprawowania przez ABI nadzoru nad dokumentacją przetwarzania danych. Sprawując nadzór ABI dokonuje weryfikacji:
– opracowania i kompletności dokumentacji przetwarzania danych;
– zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;
– stanu faktycznego w zakresie przetwarzania danych osobowych;
– zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;
– przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

ABI przeprowadza weryfikację w opisanych wyżej sprawdzeniach, a nadto, poza sprawdzeniami, na podstawie zgłoszenia osoby wykonującej obowiązki określone w dokumentacji przetwarzania danych, zgłoszenia osoby trzeciej oraz własnego udziału w procedurach określonych w dokumentacji.

W przypadku wykrycia podczas weryfikacji nieprawidłowości ABI:
– zawiadamia administratora danych o nieopracowaniu lub brakach w dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu, w szczególności może przedstawić mu do wdrożenia projekty dokumentów usuwające stan niezgodności;
– zawiadamia administratora danych o nieaktualności dokumentacji przetwarzania danych oraz może przedstawić administratorowi danych do wdrożenia projekty dokumentów aktualizujących;
– poucza lub instruuje osobę nieprzestrzegającą zasad określonych w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji lub zawiadamia administratora danych, wskazując osobę odpowiedzialną za naruszenie tych zasad oraz jego zakres; pouczenia lub instrukcje są zawarte w odrębnym dokumencie skierowanym do takiej osoby.

Realizując omawiane zadanie ABI pełni dwie funkcje:
– podmiotu nadzorującego – podejmując czynności kontrolne (sprawdzanie) oraz ewentualnie korzystając z uprawnień do pouczania lub instruowania osoby, która dopuściła się uchybień oraz
– podmiotu czynnie uczestniczącego w kreowaniu dokumentacji – poprzez przedstawianie administratorowi danych projektów dokumentów.

O pouczaniu można mówić, według mnie, w sytuacji gdy z okoliczności wynika, że osoba nieprzestrzegającą zasad określonych w dokumentacji przetwarzania danych zna te reguły lecz nie stosuje ich w praktyce, natomiast instruowanie dotyczyć ma osoby niedysponującej adekwatną wiedzą.

Zadaniem ABI jest również zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (art. 36a ust. 2 pkt 1 lit. c ustawy). Użycie przez ustawodawcę zwrotu „zapewnianie" wskazuje na traktowanie zapoznawania z przepisami jako przedsięwzięcia stałego, realizowanego w miarę potrzeb. Warto zwrócić uwagę, że spełnienie tego wymogu może nastąpić już w przypadku udostępnienia treści przepisów osobom upoważnionym do przetwarzania danych osobowych. Zatem ustawodawca nie zobowiązuje ABI do prowadzenia ani organizowania przedsięwzięć o charakterze szkoleniowym. Jak podkreśla się w doktrynie, sposób, w jaki zadanie zapewniania zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych będzie wypełniane „pozostawiono do decyzji ABI"[38]. J. Barta i in. słusznie wskazują na luki w omawianej regulacji. Obowiązki ABI nie obejmują bowiem osób, które nie posiadają aktualnie upoważnienia do przetwarzania danych (ale mają je uzyskać) oraz zapewniania zapoznania osób przetwarzających dane z dokumentacją, tj. polityką bezpieczeństwa oraz instrukcją zarządzania systemem informatycznym[39].

3. PROWADZENIE REJESTRU ZBIORÓW DANYCH PRZETWARZANYCH PRZEZ ADMINISTRATORA DANYCH JAKO ZADANIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Administrator danych, który powołał ABI i zgłosił go do rejestracji, nie podlega obowiązkowi zgłoszenia zbioru danych osobowych do rejestracji GIODO[40], z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1 ustawy (tzw. dane wrażliwe). Na podstawie art. 36a ust. 2 pkt 2 ustawy prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych zaliczone zostało do zadań ABI, z tym że podmiot ten nie prowadzi rejestru zbiorów, z obowiązku rejestracji których administratorzy danych są zwolnieni na podstawie art. 43 ust. 1 ustawy. Do administratora danych będącego adresatem decyzji o wykreśleniu ABI z rejestru, nie stosuje się zwolnienia z obowiązku zgłoszenia zbioru danych do rejestracji GIODO. Z kolei wobec administratora danych, który ponownie zgłosił do rejestracji ABI wykreślonego z rejestru na podstawie decyzji GIODO, zwolnienie z obowiązku rejestracji zbioru stosuje się po wpisaniu ponownie zgłoszonego ABI do rejestru prowadzonego przez GIODO.

Na podstawie art. 36a ust. 2 pkt 2 ustawy prowadzony przez ABI rejestr ma zawierać w odniesieniu do każdego zbioru jego nazwę, a nadto informacje wskazane w przepisach art. 41 ust. 1 pkt 2–4a i 7. Do informacji tych należą: oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania[41], cel przetwarzania danych,

---

[38] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, art. 36a, teza 7, s. 371.

[39] J.w.

[40] Jak podkreśla się w doktrynie „zwolnienie z obowiązku zgłaszania zbiorów do GIODO ma być zachętą dla administratorów danych do powoływania abi", ale „w miejsce jednego obowiązku (rejestracji zbiorów u GIODO) pojawia się inny obowiązek (rejestracji abi u GIODO)". Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, art. 36a, teza 7, s.371.

[41] W tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku powierzenia

opis kategorii osób, których dane dotyczą oraz zakres przetwarzanych danych, sposób zbierania oraz udostępniania danych, informacje o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane oraz informacje dotyczące ewentualnego przekazywania danych do państwa trzeciego.

Sposób prowadzenia przez ABI rejestru zbiorów danych określają przepisy rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r.[42] W akcie tym powtórzono za ustawodawcą wykaz informacji, dotyczących każdego zbioru, jakie ma zawierać rejestr.

ABI wpisuje zbiór danych do rejestru przed rozpoczęciem przetwarzania w zbiorze danych (podając w rejestrze datę wpisu każdego zbioru) oraz aktualizuje informacje dotyczące zbioru danych w rejestrze – w przypadku zmiany informacji objętych wpisem (podając datę ostatniej aktualizacji informacji dotyczących tego zbioru), a nadto wykreśla zbiór danych z rejestru – w razie zaprzestania przetwarzania w nim danych osobowych (pozostawiając nazwę zbioru danych, datę wpisania zbioru danych oraz datę ostatniej aktualizacji informacji dotyczących tego zbioru wraz z adnotacją, że jest to data wykreślenia zbioru z rejestru). Nadto ABI został zobowiązany do odnotowania historii zmian w rejestrze zawierającej informację o rodzaju zmiany (nowy wpis, aktualizacja, wykreślenie), jej zakresie oraz dacie jej dokonania. Barta i in. trafnie podkreślają, że „z punktu widzenia praktycznego znacznie lepszym rozwiązaniem byłoby dodanie do rozporządzenia załącznika zawierającego wzór rejestru, jaki ma prowadzić ABI. Z tej możliwości prawodawca jednak nie skorzystał”[43].

Aktualizacja informacji oraz wykreślenie zbioru danych z rejestru powinny zostać dokonane niezwłocznie po zaistnieniu zdarzenia powodującego obowiązek ich dokonania. Nietrudno zauważyć, że dokonanie wpisu zbioru do rejestru, aktualizacja informacji oraz wykreślenie zbioru będą mogły zostać przeprowadzone, jeżeli ABI otrzyma stosowną informację od podmiotów przetwarzających dane w zbiorze, bądź od administratora danych. Niestety, w przepisach ustawy oraz omawianego rozporządzenia nie wskazano na tryb informowania ABI o zdarzeniach, których zaistnienie aktualizowałoby jego obowiązki związane z prowadzeniem rejestru zbiorów. Sądzę, że procedura przekazywania ABI informacji o prowadzonych zbiorach danych osobowych oraz ich aktualizacji, jak również ewentualnym zaniechaniu przetwarzania danych w prowadzonym dotychczas zbiorze powinna stać się przedmiotem dodatkowej regulacji prawnej.

Do zadań ABI należy również udostępnianie rejestru do przeglądania. W przypadku gdy rejestr prowadzony jest w postaci papierowej, ABI udostępnia każdemu zainteresowanemu treść rejestru do przeglądania w siedzibie lub miejscu zamieszkania administratora danych. W razie prowadzenia rejestru w postaci elektronicznej, ABI udostępnia rejestr do przeglądania na stronie internetowej administratora danych[44], lub na stanowisku dostępowym w systemie informatycznym tego podmiotu znajdującym

---

przetwarzania danych podmiotowi, o którym mowa w art. 31, lub wyznaczenia podmiotu, o którym mowa w art. 31a, oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania.

[42] Dz.U. poz. 719.

[43] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, art. 36a, teza 7, s. 373.

[44] Na stronie głównej umieszcza się wówczas odwołanie umożliwiające bezpośredni dostęp do rejestru.

się w jego siedzibie lub miejscu zamieszkania, lub przez sporządzenie wydruku rejestru z systemu informatycznego administratora danych.

W przypadku prowadzenia rejestru wyłącznie w postaci elektronicznej albo w postaci papierowej i postaci elektronicznej ABI może zdecydować, że w odniesieniu do informacji określających podmiot, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy (w tym adresu jego siedziby lub miejsca zamieszkania) gromadzonych w postaci elektronicznej, udostępnia się do przeglądania wyłącznie informacje o powierzeniu przetwarzania danych innemu podmiotowi, a jego oznaczenie i adres siedziby lub miejsca zamieszkania są udostępniane jedynie do przeglądania w siedzibie lub miejscu zamieszkania administratora danych.

BIBLIOGRAFIA

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, wyd. VI – Lex, on line.

Byczkowski M., *Zapewnianie przestrzegania przepisów o ochronie danych osobowych w sferze wewnętrznej bez powołania administratora bezpieczeństwa informacji*, „Monitor Prawniczy" dodatek do nr 6/2015, s. 8–12.

Fajgielski P., *Administrator bezpieczeństwa informacji – geneza, stan obecny i perspektywy zmian*, „Monitor Prawniczy" dodatek do nr 9/2014, s. 39–44.

Fajgielski P., *Pozycja prawna i zadania administratora bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych*, „Monitor Prawniczy" dodatek do nr 6/2015, s. 3–9.

Mednis A., *Administrator bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych z 7.11.2014 r. – ocena rozwiązań*, „Monitor Prawniczy" dodatek do nr 6/2015, s. 20–25.

Pilc B., *Rola administratora bezpieczeństwa informacji podczas inspekcji prowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych*, „Monitor Prawniczy" dodatek do nr 7 z 2012 r., s. 37–42.

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. poz. 1934).

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. poz. 745).

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych, Dz.U. poz. 719.

Sibiga G., *Rejestracja administratorów bezpieczeństwa informacji. Postępowanie rejestracyjne Generalnego Inspektora Ochrony Danych Osobowych*, „Monitor Prawniczy" dodatek do nr 6/2015, s. 13–19.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, tekst jedn. Dz.U. z 2014 r. poz. 1182, ze zm.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Streszczenie

Przedmiotem artykułu jest prezentacja, analiza i ocena przepisów ustawowych oraz wykonawczych odnoszących się do powoływania, rejestracji oraz zadań administratora bezpieczeństwa informacji jako pod-miotu zobowiązanego do sprawdzania zgodności przetwarzania danych osobowych z przepisami, nadzorowania opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania takich danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, zapewniania zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ich ochronie oraz prowadzenia rejestru zbiorów danych przetwarzanych przez administratora. Przeprowadzona analiza przepisów ustawy o ochronie danych osobowych oraz rozporządzeń wykonawczych odnoszących się do administratora bezpieczeństwa informacji stanowi podstawę licznych wniosków de lege ferenda, a wśród nich m.in.: wprowadzenia obowiązku powoływania administratora bezpieczeństwa informacji przez administratora danych, wskazania w ustawie skutków prawnych: powołania administratora bezpieczeństwa informacji niespełniającego wymogów ustawowych oraz niezgłoszenia powołanego administratora bezpieczeństwa informacji do rejestracji przez Generalnego Inspektora Ochrony Danych Osobowych, jak również uregulowania w ustawie procedury przekazywania administratorowi bezpieczeństwa in-formacji wiadomości o prowadzonych zbiorach danych osobowych oraz ich aktualizacji, a także ewentualnym zaniechaniu przetwarzania danych w prowadzonym dotychczas zbiorze.

Słowa kluczowe: *Administrator bezpieczeństwa informacji*, *Administrator danych osobowych*, *GIODO*, *Ochrona danych osobowych*

ADMINISTRATOR OF DATA SECURITY

Summary

The article presents, analyses and evaluates the statutory regulations and secondary legislation on the appointment, registration and tasks of an administrator of information security as an entity obliged to check the compliance of personal data processing with the regulations, to supervise the development of and update documents describing the way of data processing and technical and organizational means ensuring the protection of personal data adequately to threats and the category of data protected, to inform persons authorized to process personal data about the provisions on their protection and to keep a register of databases processed by the administrator. The analysis of the provisions of the Act on the protection of personal data and secondary legislation on the administrator of information security constitutes basis for numerous conclusions de lege ferenda, including, inter alia, the introduction of an obligation to appoint an administrator of information security by a data administrator and pointing out legal consequences of the act in case of: an appointment of an administrator of information security who does not meet the statutory requirements and a failure to register an administrator of information security by the General Inspector of Personal Data Protection, as well as the regulation of the procedure of providing an administrator of information security with information on personal data collection and their updating as well as potential discontinuance of processing data in the existing collection.

Key words: *administrator of data security*, *administrator of personal data*, *General Inspector of Personal Data Protection*, *personal data protection*