



MINISTER KLIMATU

Michał Kurtyka

Warszawa, dnia 5.02.2020.

BAK-I.0831.3.2019.ARH

Pan
Łukasz Młynarkiewicz
p.o. Prezesa
Państwowej Agencji Atomistyki
ul. Bonifraterska 17
00-203 Warszawa

WYSTĄPIENIE POKONTROLNE

Działając na podstawie upoważnienia Ministra Środowiska¹ nr 3/2019 z 26 czerwca 2019 r. i aneksu nr 1 z 17 lipca 2019 r. zespół kontrolujący Ministerstwa Klimatu przeprowadził kontrolę w Państwowej Agencji Atomistyki (dalej: PAA/Agencja), ul. Bonifraterska 17 w Warszawie dotyczącą funkcjonowania jednostki w zakresie bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych.

Kontrola została przeprowadzona przez zespół w składzie:

- Małgorzata Keller-Boroszek – Dyrektor w Biurze Kontroli i Audytu Wewnętrznego, kierownik zespołu kontrolującego;
- Aleksandra Gregorkiewicz – Radca Ministra w Biurze Kontroli i Audytu Wewnętrznego;
- Joanna Matusiak – Główny specjalista w Biurze Kontroli i Audytu Wewnętrznego;
- Katarzyna Żebrowska – Starszy specjalista w Biurze Kontroli i Audytu Wewnętrznego;
- Mateusz Białek – Specjalista w Biurze Kontroli i Audytu Wewnętrznego.

Kontrolą objęto okres od 1 stycznia 2017 r. do 30 września 2019 r.

Kontrola została przeprowadzona na podstawie art. 25 ust. 1 pkt 3 lit. b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne² i art. 6 ust. 3 pkt 1 ustawy

¹ Zgodnie z rozporządzeniem Prezesa Rady Ministrów z 18 listopada 2019 r. - poz. 2266, od 15 listopada 2019 r. Minister Klimatu kieruje działem administracji rządowej – Środowisko. Tym samym stał się następcą prawnym Ministra Środowiska.

² t.j. Dz.U. z 2019, poz. 700 ze zm.

z dnia 15 lipca 2011 r. o kontroli w administracji rządowej³ w związku z art. 109 ust. 4 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe⁴ (dalej: prawo atomowe).

Kierownikiem jednostki kontrolowanej jest pan Łukasz Młynarkiewicz, pełniący obowiązki Prezesa PAA od 11 września 2019 r. Dotychczasowym Prezesem PAA był pan Andrzej Przybycin.⁵

W okresie objętym kontrolą Dyrektorem Generalnym PAA był pan Artur Wdowczyk⁶, odwołany ze stanowiska 20 września 2019 r. Do dnia zakończenia czynności kontrolnych tj. 30 września 2019 r. w zastępstwie Dyrektora Generalnego był pan Piotr Korzecki Dyrektor Departamentu Prawnego (dalej: Dyrektor DP wz. Dyrektora Generalnego).

[Dowód: akta kontroli str. 1, 12, 86, 105-109]

II. Wybrane zagadnienia ochrony danych osobowych, zgodnie z Rozporządzeniem 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 (ogólne rozporządzenie o ochronie danych)¹²⁷

II.1. Organizacja systemu ochrony danych osobowych

W PAA dopiero 4 lipca 2019 r., tj. po upływie ponad roku od wprowadzonego obowiązku¹²⁸ ustanowiono Politykę ochrony danych osobowych PAA¹²⁹ określającą rozwiązania organizacyjne i proceduralne dotyczące wykonywania poszczególnych obowiązków wynikających z ogólnego rozporządzenia o ochronie danych. Zgodnie z art. 24 ust. 2 ogólnego rozporządzenia o ochronie danych, jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki techniczne i organizacyjne służące ochronie danych osobowych obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Zgodnie z art. 32 ww. ogólnego rozporządzenia o ochronie danych uwzględniając stan wiedzy technicznej, koszty wdrażania oraz charakter zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator (Prezes PAA) zobowiązany jest do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym m.in. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności

¹²⁷ Dz.Urz. UE Nr L/119 z 4.5.2016 r.

¹²⁸ Od 25 maja 2018 r.

¹²⁹ Zarządzenie nr 8 Prezesa Państwowej Agencji Atomistyki z dnia 4 lipca 2019 r. w sprawie Polityki ochrony danych osobowych oraz określenia funkcji w zakresie ochrony danych osobowych w Państwowej Agencji Atomistyki.

systemów i usług przetwarzania oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Jak opisano w pkt. II.2, w PAA nie przeprowadzano analiz ryzyka naruszenia praw lub wolności osób fizycznych.

Były Dyrektor Generalny PAA odnośnie opóźnień we wdrożeniu obowiązków i zadań wynikających z ww. ogólnego rozporządzenia o ochronie danych, w tym w ustanowieniu Polityki ochrony danych osobowych wyjaśnił, że wynikały one ze zmian organizacyjnych w PAA, rezygnacji ABI z pełnienia funkcji (i konieczności wyznaczenie nowego IOD), oczekiwania na wydanie powszechnie obowiązujących przepisów mających wpływ na przetwarzanie danych osobowych, opóźnień we wdrażaniu w PAA Systemu EZD PUW, przedłużających się prac nad opracowaniem rejestru czynności przetwarzania danych w PAA¹³⁰.

Zgodnie z § 23 Polityki ochrony danych osobowych w PAA środki techniczne i organizacyjne w systemach informatycznych powinny być określone w odrębnym dokumencie dotyczącym bezpieczeństwa w obszarze IT. Środki techniczne i organizacyjne dotyczące fizycznego dostępu do obszaru, w którym przetwarzane są dane osobowe powinny być określone w regulacjach wewnętrznych Agencji.

Jako obowiązującą regulację dotyczącą bezpieczeństwa w obszarze IT były Dyrektor Generalny wskazał procedurę nr 007/BDG zarządzanie systemem informatycznym w Państwowej Agencji Atomistyki¹³¹.

[Dowód akta kontroli str. II/123-125]

Wcześniej system ochrony danych osobowych w PAA był ustanowiony Polityką bezpieczeństwa danych osobowych i ww. Instrukcją zarządzania systemem informatycznym¹³². Dodatkowo obowiązywała Instrukcja przetwarzania danych osobowych w Państwowej Agencji Atomistyki z 19 stycznia 2015 r.¹³³. Dokumenty regulujące zasady ochrony danych osobowych, obowiązujące przed 4 lipca 2019 r. były dostosowane do wymogów uchylonej¹³⁴ ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych¹³⁵ oraz uchylonego¹³⁶ Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (dalej: Rozporządzenie MSWiA)¹³⁷.

[Dowód akta kontroli str. II/24-38]

Zespół kontrolujący zwraca uwagę, że Prezes PAA w styczniu 2018 r. został poinformowany przez ABI o konieczności wdrożenia wymagań ogólnego rozporządzenia w PAA i o tym, że ABI nie jest w stanie zapewnić wykonywania swoich zadań w związku z innymi zadaniami na stanowisku prawnika.

¹³⁰ Pismo Dyrektora Generalnego PAA z dnia 9 sierpnia 2019 r.

¹³¹ Pismo z 5 września 2019 r.

¹³² Zarządzenie nr 7 Prezesa PAA z dnia 30 lipca 2014 r. w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych, Instrukcji zarządzania systemem informatycznym i Instrukcji przetwarzania danych osobowych w Państwowej Agencji Atomistyki oraz w sprawie wyznaczenia osób wykonujących zadania w zakresie ochrony danych osobowych w Państwowej Agencji Atomistyki, zmienione Zarządzeniem Nr 9 Prezesa PAA z dnia 22 września 2014 r. zmieniającym zarządzenie w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych, Instrukcji zarządzania systemem informatycznym i Instrukcji przetwarzania danych osobowych w Państwowej Agencji Atomistyki oraz w sprawie wyznaczenia osób wykonujących zadania w zakresie ochrony danych osobowych w Państwowej Agencji Atomistyki; Zarządzenie nr 2 Prezesa PAA z dnia 5 sierpnia 2015 r. w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych oraz w sprawie określenia osób wykonujących zadania w zakresie ochrony danych osobowych w Państwowej Agencji Atomistyki; Procedura nr 007/BDG z dnia 30 listopada 2017 r. – Procedura zarządzania systemem informatycznym, Załącznik nr 1 do Procedury: Instrukcja Zarządzania Systemem Informatycznym w Państwowej Agencji Atomistyki, Procedura została wprowadzona na podstawie Zarządzenia nr 2 Prezesa PAA z dnia 5 sierpnia 2015 r. w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych oraz w sprawie określenia osób wykonujących zadania w zakresie ochrony danych osobowych w Państwowej Agencji Atomistyki.

¹³³ Procedura Nr 005/GP przetwarzania danych osobowych w Państwowej Agencji Atomistyki z 19 stycznia 2015 r.

¹³⁴ Z dniem 25 maja 2018 r.

¹³⁵ Dz. U. z 2016 r. poz. 922

¹³⁶ Z dniem 25 maja 2018 r.

¹³⁷ Dz.U. 2004 nr 100 poz. 1024

Po złożeniu w grudniu 2017 r. rezygnacji przez ABI¹³⁸, ustalono, że do czasu znalezienia nowego kandydata osoba ta nadal miała wykonywać zadania ABI¹³⁹. Administrator danych mógł powierzyć ABI wykonywanie innych obowiązków, jeżeli nie naruszyło to prawidłowego wykonywania jego ustawowych zadań¹⁴⁰. Po 25 maja 2018 r., zgodnie z art. 24 ust. 2 ogólnego rozporządzenia o ochronie danych, polityki ochrony danych są wdrażane przez administratora, a IOD monitoruje ich przestrzeganie¹⁴¹. Ogólne rozporządzenie o ochronie danych jest stosowane w Państwach członkowskich bezpośrednio, bez konieczności wdrożenia jego przepisów do krajowego porządku prawnego.

[Dowód akta kontroli str. II/24-38,87-102]

Zespół kontrolujący ponadto zwraca uwagę, że obowiązująca Instrukcja zarządzania systemem informatycznym przewiduje zabezpieczenia wskazane w ww. uchylonym Rozporządzeniu MSWiA, natomiast o rodzaju i zakresie środków technicznych i organizacyjnych zgodnie z art. 32 ogólnego rozporządzenia o ochronie danych decyduje sam administrator danych na podstawie uprzednio przeprowadzonej analizy ryzyka.

Dodatkowo należy zauważyć, że obowiązująca w okresie objętym kontrolą Instrukcja przetwarzania danych osobowych w PAA zawierała część procedur opisujących sposób postępowania dla tych samych zdarzeń odmienne od procedur zawartych w Polityce ochrony danych osobowych PAA¹⁴². Oznacza to, że w tym samym czasie w PAA obowiązywały dokumenty zawierające różne procedury odnoszące się do tych samych zagadnień.

[Dowód akta kontroli str. II/39-86, II/90-95]

Kontrolujący ocenili kontrolowane zagadnienie negatywnie.

II.2 Analiza ryzyka

W PAA nie była prowadzona analiza ryzyka naruszenia praw i wolności osób fizycznych.

Zgodnie z §23 ust. 3 przyjętej w PAA, Polityki ochrony danych osobowych w PAA środki techniczne i organizacyjne w systemach informatycznych oraz dotyczące fizycznego dostępu do obszaru, w którym przetwarzane są dane osobowe, powinny zostać dobrane na podstawie przeprowadzonej analizy ryzyka.

Dyrektor Generalny PAA poinformował, że ryzyka były identyfikowane w ramach kontroli zarządczej, stosownie do postanowień Zarządzenia nr 8 Prezesa Państwowej Agencji Atomistyki w sprawie ustalenia Regulaminu kontroli zarządczej w Państwowej Agencji Atomistyki¹⁴³.

Zespół kontrolujący zwraca uwagę, że analiza ryzyka przeprowadzona w ramach kontroli zarządczej nie odnosiła się do praw i wolności osób fizycznych a jedynym ryzykiem, jakie zidentyfikowano było nieuprawnione uzyskanie dostępu do danych osobowych, a jego skutki odnosiły się do organizacji, a nie praw i wolności osób fizycznych.

W ww. analizie nie uwzględniono charakteru, zakresu, kontekstu i celu przetwarzania danych osobowych, a także ryzyka dla naruszenia praw i wolności osób fizycznych, zatem nie spełnia ona wymogów ogólnego rozporządzenia o ochronie danych.

¹³⁸ Pismo ABI do Prezesa PAA z dnia 16 stycznia 2018 r.

¹³⁹ Pismo Dyrektora Generalnego PAA z dnia 9 sierpnia 2019 r.

¹⁴⁰ art. 36a ust. 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)

¹⁴¹ art. 39 ust. 1 lit. b ogólnego rozporządzenia o ochronie danych

¹⁴² Postępowanie w przypadku wystąpienia przez osobę o informacje dotyczące przetwarzania jej danych osobowych; Postępowanie w sytuacjach naruszenia zasad ochrony danych osobowych; Nadawanie i modyfikacja uprawnień do przetwarzania danych osobowych

¹⁴³ Pismo Dyrektora Generalnego PAA z 9 sierpnia 2019 r.

Zgodnie z art. 24 ust. 1 ogólnego rozporządzenia o ochronie danych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.

Ponadto w myśl art. 32 ogólnego rozporządzenia o ochronie danych uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

W kwestii zastosowania środków bezpieczeństwa odpowiadających ryzyku Dyrektor Generalny PAA wyjaśnił, że techniczne i organizacyjne środki bezpieczeństwa opisane w rejestrze czynności przetwarzania PAA z dnia 4 lipca 2019 r. zostały dobrane na podstawie analizy dotychczas stosowanych zabezpieczeń, które okazały się skuteczne zważywszy, że nie odnotowano naruszeń praw lub wolności osób fizycznych. Biorąc pod uwagę niewielki zakres przetwarzanych danych osobowych w PAA, uwzględniając stan wiedzy technicznej, koszt wdrażania zabezpieczeń, charakter przetwarzanych danych oraz zakres, kontekst i cele przetwarzania w PAA oraz dotychczas stosowane zabezpieczenia uznano, że wdrożone w PAA środki techniczne i organizacyjne są wystarczające, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych.

Dodatkowo były Dyrektor Generalny poinformował, że kierownictwo PAA jest świadome, że istnieje praktyka dokonywania szczegółowej analizy ryzyka naruszenia praw lub wolności osób fizycznych w wyniku przetwarzania danych. W związku z powyższym postanowiono rozpocząć prace nad wprowadzeniem szczegółowej analizy ryzyka dla każdej z czynności przetwarzania, niezależnie od ryzyk identyfikowanych w ramach kontroli zarządczej¹⁴⁴.

[Dowód akta kontroli str. II/90-95]

Kontrolujący ocenili kontrolowane zagadnienie negatywnie.

II.3 Szkolenia pracowników

W PAA poza 14 pracownikami (nie licząc IOD) nie zapewniono przeszkolenia pracowników z zakresu ogólnego rozporządzenia o ochronie danych osobowych.

Inspektor Ochrony Danych prowadził szkolenia wstępne przed rozpoczęciem wykonywania obowiązków służbowych przez pracowników¹⁴⁵.

[Dowód akta kontroli str. II/132-143]

Zastępca Dyrektora Departamentu Budżetowo-Organizacyjnego wyjaśnił, że szkolenie okresowe z zakresu ochrony danych osobowych było planowane na październik 2018 r. Z uwagi na zmiany organizacyjne w PAA nie doszło jednak do skutku. Pracownicy PAA byli kierowani na szkolenia z zakresu ochrony danych osobowych na podstawie indywidualnych wniosków, po uzyskaniu zgody Dyrektora Generalnego¹⁴⁶.

¹⁴⁴ Pismo Dyrektora Generalnego PAA z 9 sierpnia 2019 r.

¹⁴⁵ Pismo IOD z 20 września 2019 r.

¹⁴⁶ Pismo Zastępcy Dyrektora Departamentu Budżetowo-Organizacyjnego z 12 sierpnia 2019 r.

Zespół kontrolujący zwraca uwagę, że przeszkolenie pracowników było wskazane z uwagi na zmiany w przepisach dotyczących ochrony danych osobowych i wzrost odpowiedzialności administratora za ochronę i prawidłowość przetwarzania danych.

[Dowód akta kontroli str. 224-250, II/130-131]

Kontrolujący ocenili kontrolowane zagadnienie pozytywnie, rekomendując jednocześnie objęcie wszystkich pracowników szkoleniem w zakresie ochrony danych osobowych.

II.4 Upoważnienia do przetwarzania danych osobowych

Wszyscy pracownicy PAA otrzymali imienne upoważnienie do przetwarzania danych osobowych od Administratora danych. Inspektor Ochrony Danych prowadził ewidencję upoważnień do przetwarzania danych osobowych. Procedura postępowania w zakresie udzielania upoważnienia do przetwarzania danych osobowych w PAA została opisana w Polityce ochrony danych osobowych PAA z dnia 4 lipca 2019 r.

[Dowód akta kontroli str. II/39-71, 144]

Kontrolujący ocenili kontrolowane zagadnienie pozytywnie.

II.5 Przetwarzanie danych przez podmioty przetwarzające

W PAA dokonano inwentaryzacji umów powierzenia. Prowadzony jest również ich rejestr. Według stanu na dzień 9 sierpnia 2019 r. w rejestrze zarejestrowano 5 umów powierzenia (w przypadku dwóch umów PAA było podmiotem przetwarzającym). Postępowanie w zakresie zawierania umów lub porozumień w sprawie powierzenia przetwarzania danych osobowych reguluje Polityka ochrony danych osobowych PAA z dnia 4 lipca 2019 r.

[Dowód akta kontroli str. II/39-71, 145-151, 184-194]

Kontrola ¹⁴⁷ umów powierzenia danych pomiędzy PAA, jako Administratorem danych a podmiotami przetwarzającymi wykazała, że w dwóch przypadkach umowy zostały zawarte zgodnie z obowiązującymi regulacjami wewnętrznymi. Badanie dwóch pozostałych umów powierzenia wykazało, że:

- jedna z nich została zawarta przez osobę, której administrator nie udzielił pisemnego pełnomocnictwa do jej zawarcia oraz w jej zapisach nie dookreślono udzielenia zgody albo jej braku na korzystanie z innych podmiotów przetwarzających oraz nie zobowiązano podmiotu przetwarzającego do udostępnienia administratorowi danych wszelkich informacji niezbędnych do wykazania obowiązków wynikających z art. 28 ogólnego rozporządzenia¹⁴⁸,
- jedna została zawarta dopiero po 8 miesiącach¹⁴⁹ od zawarcia umowy serwisowej¹⁵⁰ na sprawowanie nadzoru autorskiego i opieki autorskiej nad oprogramowaniem autorskim, wspieranie użytkowników i wykonywanie serwisu eksploatacyjnego tego oprogramowania (26 sierpnia 2019 r.). W systemie kadrowo-płacowym były przetwarzane dane osobowe m.in. pracowników PAA.

[Dowód akta kontroli str. II/152-165]

¹⁴⁷ Jednej z umów nie ujęto w rejestrze umów powierzenia, ponieważ była zawarta po jego przekazaniu zespołowi kontrolującemu

¹⁴⁸ Umowa powierzenia z 25 maja 2018 r.

¹⁴⁹ 26 sierpnia 2019 r.

¹⁵⁰ nr 2/F/2019/5 z 19 grudnia 2018 r.

Zgodnie z art. 28 ust. 3 ogólnego rozporządzenia o ochronie danych, przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Zgodnie z art. 4 pkt. 7 administratorem danych jest m.in. organ publiczny, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Art. 28 ust. 3 lit. d oraz h stanowią, że przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy, która stanowi w szczególności, że podmiot przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4 art. 28 i udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28.

Zastępca Dyrektora Departamentu Budżetowo-Organizacyjnego wyjaśnił, że opóźnienie w zawarciu umowy powierzenia na nowych warunkach wynikało z przedłużających się negocjacji treści umowy powierzenia. Ponieważ zgodnie z wolą stron, umowa główna z 2018 r. była kontynuowana w 2019 r., według Zastępcy Dyrektora należy uznać, że umowa o powierzenie przetwarzania danych osobowych z 25 maja 2018 r. została przedłużona w sposób dorozumiany poprzez jej wykonywanie do dnia zawarcia nowej umowy powierzenia (na podstawie § 10 ust. 2 umowy z dnia 25 maja 2018 r. w zw. z art. 60 kodeksu cywilnego¹⁵¹).

[Dowód akta kontroli str. II/126-129]

Dyrektor Departamentu Prawnego wyjaśnił, że umowa powierzenia dotyczyła danych osobowych głównie pracowników PAA. Ze względu na charakter danych osobowych, które zostały powierzone na podstawie przedmiotowej umowy uznano ówczesnie, że administratorem danych w zakresie objętym umową jest Dyrektor Generalny PAA wykonujący zadania określone w art. 25 ust. 4 ustawy o służbie cywilnej. Dyrektor podniósł też, że fakt podpisania umowy powierzenia przez Dyrektora Generalnego nie był kwestionowany przez Prezesa Państwowej Agencji Atomistyki¹⁵².

[Dowód akta kontroli str. II/166-168]

Zespół kontrolujący zwraca uwagę, że Administratorem danych jest Prezes Państwowej Agencji Atomistyki, co znalazło także odzwierciedlenie w regulacjach wewnętrznych PAA. Zatem przedmiotowa umowa powinna być zawarta przez Prezesa PAA lub osobę przez niego upoważnioną.

Umowa powierzenia z dnia 25 maja 2018 r. zgodnie z zapisami §7 ust. 1, została zawarta na okres od dnia 25 maja 2018 r. do dnia 31 grudnia 2018 r. Zgodnie z §10 ust. 2 umowy powierzenia, w sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego, ogólnego rozporządzenia o ochronie danych osobowych oraz inne przepisy krajowe dotyczące ochrony danych osobowych. Okres obowiązywania umowy powierzenia został w niej wyraźnie uregulowany, zatem § 10 ust. 2 nie ma w tym przypadku zastosowania.

Brak zawarcia umowy powierzenia przez 8 miesięcy w sytuacji, gdy podmiot zewnętrzny wykonywał usługi na rzecz administratora danych oraz zawarcie umowy przez osobę bez pełnomocnictwa było działaniem niezgodnym z przepisami prawa oraz regulacjami wewnętrznymi.

Kontrolujący ocenili kontrolowane zagadnienie negatywnie.

¹⁵¹ Pismo z 18 września 2019 r.

¹⁵² Pismo Dyrektora Departamentu Prawnego PAA z 25 września 2019 r.

II.6 Prawo do przetwarzania danych osobowych

Dla wszystkich zbiorów danych/czynności przetwarzania danych osobowych w PAA zidentyfikowano podstawę prawną ich przetwarzania, co udokumentowano w rejestrze czynności przetwarzania danych osobowych i rejestrze kategorii czynności przetwarzania, przy czym rejestry te zostały zatwierdzone dopiero 4 lipca 2019 r. tj. z ponad rocznym opóźnieniem od daty wprowadzonego obowiązku (25 maja 2018 r.).

W PAA zidentyfikowano 51 czynności przetwarzania danych osobowych. W ramach kontroli zweryfikowano przetwarzanie danych osobowych dla 4 czynności (7,8% wszystkich czynności przetwarzania), tj.:

1. Przesyłanie wniosków kandydatów na stypendia naukowe, wizyty naukowe, kursy szkoleniowe, wyjazdy konsultantów, seminaria, konferencje.
2. Prowadzenie centralnego rejestru dawek indywidualnych.
3. Przeprowadzanie egzaminów na stanowiska mające istotne znaczenie dla zapewnienia bezpieczeństwa jądrowego i ochrony radiologicznej oraz uprawnienia inspektorów ochrony radiologicznej.
4. Prowadzenie rejestrów osób fizycznych posiadających uprawnienie do pracy na stanowisku mającym istotne znaczenie dla zapewnienia bezpieczeństwa jądrowego i ochrony radiologicznej oraz uprawnienia inspektorów ochrony radiologicznej.

[Dowód akta kontroli str. II/195-204]

We wszystkich przypadkach stwierdzono: spełnienie warunków przetwarzania, określonych w podstawie prawnej przetwarzania i zawartej w rejestrze czynności; zgodność celów przetwarzania z celami, w jakich dane zostały zebrane; przetwarzanie danych wyłącznie w zakresie niezbędnym do realizacji celów ich przetwarzania; przetwarzanie danych w formie umożliwiającej identyfikację osoby, której dane dotyczą.

[Dowód akta kontroli str. II/205-472]

Kontrolujący ocenili kontrolowane zagadnienie pozytywnie.

II.7 Realizacja praw osób, których dane dotyczą

Procedura realizacji praw osób, których dane dotyczą została opisana w Polityce ochrony danych osobowych PAA. Określono także osoby odpowiedzialne za realizację praw osób. Opracowano wzory klauzul informacyjnych zgodnych z art. 13 i 14 ogólnego rozporządzenia o ochronie danych. Klauzule te jednak nie zawierają informacji o ewentualnym zamiarze przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowej i podjętych zabezpieczeniach w tym zakresie, co jest wymogiem art. 13 ust. 1 lit. f oraz art. 14 ust. 1 lit. f ogólnego rozporządzenia o ochronie danych.

Procedura udzielania informacji z art. 13 i 14 ogólnego rozporządzenia o ochronie danych nie przewiduje obowiązku ponownego zastosowania klauzuli informacyjnej wobec osób, których dane osobowe zostały zebrane w innym celu niż zamierzony cel ich wykorzystania.

Zgodnie z art. 12 ust. 3 ogólnego rozporządzenia o ochronie danych Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.

Procedura opisana w Załączniku nr 6 Postępowanie dotyczące wniosku złożonego przez osobę w zakresie przysługujących jej praw, do Polityki ochrony danych osobowych PAA nie zawiera zapisów, zgodnie z którymi administrator udziela osobie informacji o działaniach podjętych w związku z jej żądaniem w terminie miesiąca od otrzymania żądania, a w razie potrzeby o przedłużeniu tego terminu o kolejne 2 miesiące.

[Dowód akta kontroli str. II/39-71]

W okresie objętym kontrolą do PAA nie wpłynęły wnioski o realizację praw osób, których dane dotyczą.

[Dowód akta kontroli str. II/90-95]

W ramach skontrolowanych czynności przetwarzania danych osobowych spełniano obowiązek informacyjny, o którym mowa w art. 13 ogólnego rozporządzenia o ochronie danych z jednym wyjątkiem. Nie przekazywano klauzuli informacyjnej zawierającej wszystkie informacje wymagane art. 13 ogólnego rozporządzenia o ochronie danych wszystkim osobom, których dane są przetwarzane w Departamencie Ochrony Radiologicznej (dalej: DOR), w związku z przeprowadzaniem egzaminów na stanowiska mające istotne znaczenie dla zapewnienia bezpieczeństwa jądowego i ochrony radiologicznej oraz uprawnienia inspektorów ochrony radiologicznej oraz prowadzeniem rejestru osób fizycznych posiadających uprawnienia do pracy na stanowisku mającym istotne znaczenie dla zapewnienia bezpieczeństwa jądowego i ochrony radiologicznej oraz uprawnienia inspektorów ochrony radiologicznej.

Osoby, które przystępują do egzaminu na nadanie uprawnień, a których dane są przetwarzane w ramach ww. czynności przetwarzania podpisują oświadczenie na których wyrażają zgodę na przetwarzanie danych osobowych oraz, że są świadomi tożsamości administratora danych, celu zbierania danych, prawie dostępu do danych oraz możliwości ich skorygowania, oraz o obowiązku podania danych, który wynika z § 12 ust. 1 Rozporządzenia Rady Ministrów z dnia 2 września 2016 r. w sprawie stanowiska mającego istotne znaczenie dla zapewnienia bezpieczeństwa jądowego i ochrony radiologicznej oraz inspektorów ochrony radiologicznej.

[Dowód akta kontroli str. II/361-472]

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych, podczas pozyskiwania danych osobowych należy wypełnić obowiązek informacyjny wobec osoby, której dane są zbierane. Zakres podanych informacji precyzuje ust. 1 i 2 tegoż artykułu. Zakres informacji podanych w ww. oświadczeniu zawężono w stosunku do zakresu informacji wymaganych w art. 13.

Przetwarzanie danych w ramach powyższych czynności przetwarzania odbywa się na podstawie art. 6 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych¹⁵³ w związku z ustawą z dnia 29 listopada 2000 r. Prawo atomowe¹⁵⁴.

W wymaganych przez PAA oświadczeniach dotyczących m.in. przetwarzania danych, osoby wyrażają zgodę na przetwarzanie danych osobowych. Zespół kontrolujący zwraca uwagę, że przyjęty przez PAA sposób postępowania wprowadza osobę składającą oświadczenie w błąd, co do podstawy przetwarzania jej danych osobowych, na którą jak wynika z oświadczenia jest wyrażona zgoda, w sytuacji, gdy podstawą jest przepis prawa.

Kontrolowany zakres oceniono pozytywnie z zastrzeżeniami.

¹⁵³ przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze

¹⁵⁴ Dz. U. z 2001 r. Nr 3, poz. 18 z późn. zm.

II.8 Inspektor ochrony danych

W PAA został powołany Inspektor Ochrony Danych w terminie wynikającym z ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Dopelniono ustawowego obowiązku zawiadomienia PUODO o powołaniu IOD. Dane kontaktowe do IOD zostały upublicznione na stronie internetowej PAA.

IOD jest bezpośrednio podległy najwyższemu kierownictwu jednostki tj. Prezesowi PAA – Administratorowi danych. Osoba pełniąca funkcję IOD wykonuje inne zadania na podstawie opisu stanowiska pracy, które nie powodują konfliktu interesów z funkcją IOD. Osoba ta nie zajmuje stanowiska kierowniczego. IOD posiada doświadczenie i wykształcenie niezbędne do pełnienia tej funkcji. Na podstawie Polityki ochrony danych PAA, IOD ma możliwość włączenia się we wszystkie procesy przetwarzania danych w PAA.

[Dowód akta kontroli str. II/478-509]

Kontrolujący ocenili kontrolowane zagadnienie pozytywnie.

II.9 Rejestrowanie czynności przetwarzania danych osobowych

Rejestr czynności przetwarzania PAA oraz Rejestr kategorii czynności przetwarzania zostały zatwierdzone dopiero 4 lipca 2019 r., tj. ponad rok po wejściu w życie ogólnego rozporządzenia o ochronie danych. Rejestry zawierają wszystkie elementy wymagane przez art. 30 ust. 1 ogólnego rozporządzenia o ochronie danych. W trakcie kontroli Dyrektor Generalny wyjaśniał, m.in. że przyczyną niezakończenia prac nad Polityką ochrony danych osobowych PAA w terminie wejścia w życie ogólnego rozporządzenia o ochronie danych spowodowane były m.in. przedłużające się prace nad opracowaniem rejestru czynności przetwarzania danych w PAA.

[Dowód akta kontroli str. II/195-204]

Zgodnie z art. 30 ogólnego rozporządzenia o ochronie danych każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada, a podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.

Odnosnie przyczyn opóźnienia w zatwierdzeniu rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania były Dyrektor Generalny PAA wyjaśnił, że powyższe spowodowane było zmianami organizacyjnymi w PAA na początku 2019 r. Dodatkowo poinformował, że rejestr kategorii przetwarzania przed jego formalnym zatwierdzeniem był prowadzony przez ABI i IOD w formie elektronicznej¹⁵⁵.

[Dowód akta kontroli str. II/90-95]

Kontrolujący ocenili kontrolowane zagadnienie negatywnie.

Naruszenia ochrony danych

W PAA nie stwierdzono incydentów naruszenia ochrony danych osobowych¹⁵⁶. Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych została opisana w Polityce ochrony danych osobowych PAA.

[Dowód akta kontroli str. II/39-71, 510]

¹⁵⁵ Pismo Dyrektora Generalnego PAA z 9 sierpnia 2019 r.

¹⁵⁶ Pismo PAA z 9 sierpnia 2019 r.

Ocena obszaru

Kontrolowane zagadnienia zostają ocenione negatywnie.

W PAA do dnia 25 maja 2018 r. nie ustanowiono systemu ochrony danych zgodnego z ogólnym rozporządzeniem o ochronie danych. Nie została przeprowadzona analiza ryzyka naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych w PAA. Nie sporządzono także rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania w wymaganym terminie. Polityka ochrony danych osobowych PAA oraz rejestry czynności zostały zatwierdzone dopiero 4 lipca 2019 r. System organizacyjny ochrony danych wdrożony 4 lipca 2019 r. jest zgodny z wymaganiami ogólnego rozporządzenia o ochronie danych. Niemniej wdrożone zabezpieczenia techniczne i organizacyjne nie zostały poprzedzone analizą ryzyka. W szkoleniach z ochrony danych osobowych uczestniczyli jedynie wybrani pracownicy PAA, nie zorganizowano szkolenia dla wszystkich pracowników przetwarzających dane osobowe.

Jedna z umów powierzenia została zawarta przez Dyrektora Generalnego PAA bez posiadania stosownego pełnomocnictwa. W jednej czynności przetwarzania danych nie jest przekazywana osobom klauzula informacyjna zawierająca wszystkie wymagane elementy, a osoby wyrażają zgodę na przetwarzanie danych osobowych, mimo faktu, że przetwarzanie danych odbywa się na podstawie przepisów prawa.

W przypadku skontrolowanych czynności przetwarzania danych spełniono warunki przetwarzania, określone w podstawie prawnej przetwarzania, zawartej w rejestrze czynności, dane są przetwarzane w celach, w jakich zostały zebrane, w sposób adekwatny, w formie umożliwiającej identyfikację osoby, której dane dotyczą. Jest wypełniany obowiązek informacyjny wobec osób, których dane są zbierane, z wyjątkiem jednej czynności przetwarzania.

Administrator danych wyznaczył IOD w ustawowym terminie. Osoba ta posiada niezbędne wiedzę i doświadczenie. Podlega bezpośrednio pod kierownika jednostki i wykonuje swoje zadania niezależnie.

Przedstawiając powyższe wystąpienie pokontrolne, proszę Pana Prezesa o złożenie pisemnej informacji w sprawie sposobu wykorzystania wyników kontroli oraz o podjętych działaniach zmierzających do realizacji zaleceń pokontrolnych wraz ze stosownymi dokumentami potwierdzającymi podjęte działania—w terminie 1 miesiąca od daty otrzymania niniejszego pisma.

Z poważaniem


MINISTER KLIMATU
Michał Kurtyka

Do wiadomości:

Pan _____ – Dyrektor Biura Ministra