BIURO
GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH

Departament Inspekcji

Zestawienie wyników kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzonych w kancelariach prawnych.

Warszawa, 2017 r.

I. Wprowadzenie

Przedmiot kontroli: zbadanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), zwaną dalej „ustawą", oraz rozporządzeniem 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 (Dz. U. Nr 100, poz. 1024), zwanym dalej „rozporządzeniem".

Cel przeprowadzenia kontroli: ustalenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przez kancelarie prawne.

Zakres kontroli: zabezpieczenie oraz udostępnianie przez kancelarie prawne, danych osobowych klientów, poprzez ustalenie m.in.:

1. W jaki sposób są zbierane i udostępniane dane osobowe.
2. Czy przetwarzanie danych osobowych jest powierzane innym podmiotom (art. 31 ustawy).
3. Czy przetwarzane są dane powierzone przez inne podmioty.
4. Czy zostały zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności, czy dane zostały zabezpieczone przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy).
5. Czy prowadzona jest dokumentacja opisująca sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy (art. 36 ust. 2 ustawy).
6. Czy powołany został administrator bezpieczeństwa informacji (art. 36a ust. 1 ustawy).
7. Czy osobom dopuszczonym do przetwarzania danych osobowych zostały nadane upoważnienia do ich przetwarzania (art. 37 ustawy).
8. W jaki sposób realizowany jest obowiązek zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38 ustawy).
9. Czy prowadzona jest ewidencja osób upoważnionych do przetwarzania danych zgodnie z art. 39 ustawy.
10. Czy systemy informatyczne spełniają wymogi określone w rozporządzeniu.

Kontrole zostały podjęte z inicjatywy własnej Generalnego Inspektora Ochrony Danych Osobowych, zgodnie z planem kontroli sektorowych na 2016 r.

Czynności kontrolne przeprowadzono od września do grudnia 2016 r.

Kontrole zostały przeprowadzone: w wybranych dziesięciu (10) kancelariach prawnych, w tym dwóch (2) kancelariach prowadzonych przez adwokatów, sześciu (6) kancelariach prowadzonych przez radców prawnych i dwóch (2) kancelariach prowadzonych w formie spółki z ograniczoną odpowiedzialnością.

II. Istotne ustalenia kontroli

1. Inspektorzy GIODO ustalili, że kancelarie prawne świadczą usługi prawne realizowane przez adwokatów i radców prawnych wspomaganych przez aplikantów adwokackich, aplikantów radcowskich oraz innych upoważnionych pracowników, w tym pracowników sekretariatów.
2. Kancelarie prawne przetwarzają dane osobowe klientów w oparciu o powszechnie obowiązujące przepisy prawa, tj. przepisy ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. z 2015 r. poz. 615) oraz ustawy z dnia 6 lipca 1982 r. o radcach prawnych (Dz. U. z 2015 r. poz. 507 ze zm.), a także na podstawie przepisów korporacyjnych wydanych przez samorząd zawodowy adwokatury lub samorząd radców prawnych.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.) w a**rt. 17 ust. 1**[1] daje możliwość tworzenia w drodze ustawy samorządów zawodowych, reprezentujących osoby wykonujące zawody zaufania publicznego i **sprawowania przez te samorządy pieczy nad należytym wykonywaniem tych zawodów**. Uprawnienie do opracowania i wdrożenia przez samorząd adwokacki przepisów korporacyjnych wynika z **art. 3 ust. 1 pkt 5 ustawy Prawo o adwokaturze**[2]**,** natomiast uchwalenie przez samorząd radców prawnych zasad etyki radców prawnych wynika z **art. 57 pkt 7 ustawy o radcach prawnych**[3].
3. Kancelarie prawne świadczą usługi prawne m.in. klientom indywidualnym (osobom fizycznym). W związku ze świadczonymi usługami z klientem zawierana jest pisemna umowa o świadczenie pomocy prawnej[4], bądź ustna – w przypadku jeżeli udzielana jest tylko porada prawna; dodatkowo,

[1] Art. 17 ust. 1 Konstytucji Rzeczypospolitej Polskiej. W drodze ustawy można tworzyć samorządy zawodowe, reprezentujące osoby wykonujące zawody zaufania publicznego i sprawujące pieczę nad należytym wykonywaniem tych zawodów w granicach interesu publicznego i dla jego ochrony.
[2] Art. 3 ust. 1 pkt 5 ustawy Prawo o adwokaturze. Zadaniem samorządu zawodowego adwokatury jest ustalanie i krzewienie zasad etyki zawodowej oraz dbałość o ich przestrzeganie.
[3] Art. 57 ustawy o radcach prawnych. Do Krajowego Zjazdu Radców Prawnych należy uchwalanie zasad etyki radców prawnych.
[4] Art. 25 ust. 1 ustawy Prawo o adwokaturze. Umowę z klientem zawiera kierownik zespołu adwokackiego w imieniu zespołu; pełnomocnictwa klient udziela adwokatowi.

gdy klient ma być reprezentowany przez adwokat lub radcę prawnego przed sądem, klient udziela pełnomocnictwa procesowego.

4. Dokumentację zawierającą dane osobowe klientów przekazują kancelarii sami klienci bezpośrednio podczas spotkań z adwokatami (aplikantami adwokackimi), radcami prawnymi (aplikantami radcowskimi) lub przesyłają dokumenty zawierające dane osobowe klientów pocztą tradycyjną bądź za pośrednictwem poczty elektronicznej na służbowe skrzynki mailowe adwokatów lub radców prawnych.

5. Dokumentację klienta stanowią akta sprawy, które - jak wykazały ustalenia kontroli - zabezpieczane były przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną.

6. W wyniku kontroli inspektorzy ustalili, że dane osobowe klientów kancelarii przetwarzane były w przeważającej większości przypadków w systemach informatycznych, służących do tworzenia i edycji tekstów oraz do tworzenia arkuszy kalkulacyjnych. Niejednokrotnie korespondencja z klientami prowadzona była za pośrednictwem poczty elektronicznej. W jednym przypadku skrzynki poczty elektronicznej kancelarii były ulokowane na serwerze pocztowym, którego właścicielem jest podmiot z siedzibą w Stanach Zjednoczonych. Kancelarie prawne korzystały także z usług poczty elektronicznej świadczonych przez innych dostawców.

III. Zagadnienia problemowe

1. Adwokat i radca prawny obowiązani są do zachowania w tajemnicy wszystkiego, o czym dowiedzieli się w związku z udzielaniem pomocy prawnej (art. 6 ust. 1 ustawy Prawo o adwokaturze, oraz art. 3 ust. 3 ustawy o radcach prawnych).

Szczególnym zainteresowaniem inspektorów zostało objęte ustalenie podstawy prawnej dostępu do danych klientów objętych tajemnicą adwokacką oraz tajemnicą radcowską przez inne osoby niż adwokat i radca prawny posiadające wgląd w dane, w związku z wykonywaniem obowiązków służbowych w kancelariach prawnych.

Kontrole wykazały, że osoby zatrudnione w kancelariach przy przetwarzaniu danych upoważnione zostały do przetwarzania danych osobowych (art. 37 ustawy[5]) i zobowiązane do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczenia (art. 39 ust. 2 ustawy[6]).

Ponadto, wskazać należy, że zarówno samorząd adwokacki, jak i samorząd radców prawnych opracował i wdrożył przepisy korporacyjne, do których należy m.in. Regulamin wykonywania zawodu adwokata w kancelarii indywidualnej lub spółkach (obwieszczenie Prezydium Rady

[5] Art. 37 ustawy. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

[6] Art. 39 ust. 2 ustawy. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Adwokackiej z dnia 7 lipca 2015 r. w sprawie ogłoszenia jednolitego tekstu Regulaminu wykonywania zawodu adwokata w kancelarii indywidualnej lub spółkach) oraz Kodeks Etyki Radcy Prawnego wprowadzony uchwałą nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z dnia 22 listopada 2014 r. w sprawie Kodeksu Etyki Radcy Prawnego.

Z treści ww. regulacji wynika obowiązek przyjęcia od osób niebędących adwokatami, aplikantami adwokackimi, radcami lub aplikantami radcowskimi oświadczenia o zobowiązaniu do przestrzegania tajemnicy adwokackiej czy radcowskiej w zakresie nie mniejszym niż ten, w jakim tajemnica wiąże adwokata, czy radcę prawnego (§ 1 pkt 16 Regulaminu wykonywania zawodu adwokata w kancelarii indywidualnej lub spółkach[7], art. 22 Kodeksu Etyki Radcy Prawnego[8]). Także administrowanie systemem informatycznym przez osoby trzecie i zlecanie określonych czynności innym niż adwokat, aplikant adwokacki, radca lub aplikant radcowski osobom wiąże się z jednoczesnym zobowiązaniem tych osób do przestrzegania tajemnicy prawnie chronionej, w zakresie nie mniejszym niż ten, w jakim tajemnica wiąże adwokata, czy radcę prawnego (§ 5 ust. 4 Regulaminu wykonywania zawodu adwokata w kancelarii indywidualnej lub spółkach[9], art. 23 Kodeksu Etyki Radcy Prawnego[10]).

Inspektorzy ustalili także, że kancelarie prawne powierzają innym podmiotom przetwarzanie danych osobowych (art. 31 ustawy o ochronie danych osobowych), zlecając takie czynności, jak utrzymywanie serwerów służących do obsługi poczty elektronicznej, wykonanie i serwisowanie systemów informatycznych, prowadzenie ksiąg rachunkowych, prowadzenie i przechowywanie dokumentacji podatkowej oraz niszczenie dokumentacji.

W większości przypadków powierzenie przetwarzania danych odbywało się w oparciu o umowy zawarte z tymi podmiotami, zawierające postanowienia odnośnie zakresu i celu przetwarzania danych osobowych oraz zobowiązanie do podjęcia przed przystąpieniem do

[7] § 1 pkt 16 Regulaminu wykonywania zawodu adwokata w kancelarii indywidualnej lub spółkach. Adwokat zatrudniający osoby nie będące adwokatami, aplikantami adwokackimi, radcami lub aplikantami radcowskimi **lub zlecający określone czynności takim osobom,** przed udostępnieniem takim osobom danych objętych tajemnicą zawodową adwokata uzyskuje od takich osób na piśmie zobowiązanie do przestrzegania tej tajemnicy w zakresie nie mniejszym niż ten, w jakim tajemnica wiąże adwokata.

[8] Art. 22 **Kodeksu Etyki Radcy Prawnego.** Radca prawny powinien wyraźnie zobowiązać osoby współpracujące z nim przy wykonywaniu czynności zawodowych do zachowania poufności w zakresie objętym jego tajemnicą zawodową, wskazując na ich odpowiedzialność prawną związaną z ujawnieniem tajemnicy zawodowej.

[9] § 5 ust. 4 Regulaminu wykonywania zawodu adwokata w kancelarii indywidualnej lub spółkach. Korespondencja prowadzona w formie elektronicznej musi być zabezpieczona przed dostępem osób spoza kancelarii lub spółki, **co nie stoi na przeszkodzie zlecaniu czynności administrowania systemem informatycznym przez osoby trzecie.** Postanowienia § 1 ust. 16 stosuje się odpowiednio.

[10] Art. 23 **Kodeksu Etyki Radcy Prawnego.** Radca prawny obowiązany jest zabezpieczyć przed niepowołanym ujawnieniem wszelkie informacje objęte tajemnicą zawodową, niezależnie od ich formy i sposobu utrwalenia. Dokumenty i nośniki zawierające informacje poufne należy przechowywać w sposób chroniący je przed zniszczeniem, zniekształceniem lub zaginięciem. Dokumenty i nośniki przechowywane w formie elektronicznej powinny być objęte odpowiednią kontrolą dostępu oraz zabezpieczeniem systemu przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych. Radca prawny powinien kontrolować dostęp osób współpracujących do takich dokumentów i nośników.

przetwarzania danych osobowych środków zabezpieczających, o których mowa w art. 36-39 ustawy oraz dotyczące spełniania wymagań określonych w rozporządzeniu.

2. Inspektorzy GIODO w toku kontroli, zwrócili również uwagę na sposób zabezpieczania danych osobowych przesyłanych w formie załączników za pośrednictwem skrzynki poczty elektronicznej. Ustalono m.in., że pliki załączników do poczty elektronicznej przesyłane przez kancelarie, co do zasady, były zabezpieczane, jednakże z uwagi na zagrożenia bezpieczeństwa danych, w tym korzystanie z chmury obliczeniowej, należało zwrócić uwagę na następujące kwestie.

Z uwagi na specyfikę działania poczty elektronicznej, przesyłanie danych osobowych za jej pośrednictwem poprzez sieć publiczną (Internet) bez zastosowania odpowiednich zabezpieczeń może skutkować zagrożeniem poufności korespondencji. Do zagrożeń należy m. in. możliwość „podsłuchu" w sieci, a także podglądu korespondencji przez operatorów serwerów pocztowych i innych urządzeniach pośredniczących podczas jej przechowywania w systemie pocztowym i urządzeniach pośredniczących (podczas przesyłania przesyłki od nadawcy do odbiorcy może ona przechodzić przez wiele urządzeń pośredniczących w węzłach sieciowych). Poza przesłaniem przesyłki, serwery poczty elektronicznej przechowują treść przesyłki do chwili jej usunięcia (skąd mogą zostać skopiowane na **lokalnym nośniku w** celu dalszego jej przeglądania).

Kolejnym zagrożeniem jest możliwość ujawnienia informacji podczas działania niektórych programów pocztowych, które po wystąpieniu błędu, mogą tworzyć raport z jego wystąpienia i automatycznie przesyłać go do działu wsparcia technicznego producenta programu. Łącznie z raportem jest zwykle dostarczana część przesyłki, która spowodowała błąd.

Zaszyfrowanie dołączanych do wiadomości załączników, przesyłanych za pośrednictwem poczty elektronicznej, może uchronić kancelarię prawną przed udostępnieniem danych osobie nieupoważnionej, np. w przypadku pomyłki w adresie poczty elektronicznej odbiorcy, do którego wysyłana jest wiadomość elektroniczna.

Globalni dostawcy usług poczty elektronicznej bez przeszkód mogą przemieszczać i powielać dane między swoimi serwerami, aby skorzystać z mniej obciążonych serwerów zlokalizowanych w różnych strefach czasowych czy z dostępności taniej energii elektrycznej (zwłaszcza zmieniających się zasobów odnawialnych) oraz poprawić wyniki i zwiększyć elastyczność. W związku z tym, należy mieć na względzie, że dostęp do danych przetwarzanych na serwerach wykorzystywanych do świadczenia usług poczty elektronicznej mogą uzyskiwać także podmioty

uprawnione na podstawie przepisów prawa obowiązujących w miejscach, gdzie ulokowane są serwery[11].

Wymogi dotyczące konieczności zabezpieczenia danych przesyłanych za pośrednictwem poczty elektronicznej potwierdzone zostały w dobrych praktykach dotyczących bezpieczeństwa informacji, zawartych m.in. w normie PN-ISO/IEC 27002:2013. W rozdziale 13.2 ww. normy, dotyczącym przesyłania informacji, zaleca się wdrożenie formalnych polityk przesyłania informacji, procedur i zabezpieczeń w celu ochrony informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności. Zaleca się, aby procedury i zabezpieczenia stosowane w przypadku przesyłania informacji z użyciem środków komunikacji uwzględniały w szczególności:

1) ochronę przesyłanej informacji przed przechwyceniem, kopiowaniem, modyfikacją, błędnym routingiem i zniszczeniem;
2) ochronę wrażliwych informacji elektronicznych przekazywanych w formie załączników;
3) korzystanie z technik kryptograficznych, np. do ochrony poufności, integralności i autentyczności informacji.

Także w jednej ze spraw prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych została wydana decyzja administracyjna (sygn. decyzji DIS/DEC-13/1114/11), w której nakazano administratorowi danych, usunięcie uchybień w procesie przetwarzania danych osobowych poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przesyłanych za pośrednictwem poczty elektronicznej poprzez wprowadzenie mechanizmu szyfrowania danych przesyłanych w sieci publicznej.

Należy wziąć również pod uwagę, iż decydując się na wykorzystanie usług poczty elektronicznej oferowanych przez podmioty zewnętrzne, zazwyczaj będzie dochodzić do przetwarzania danych osobowych w tzw. chmurze obliczeniowej. Chmura obliczeniowa jest modelem umożliwiającym powszechny, wygodny, udzielany na żądanie za pośrednictwem sieci dostęp do wspólnej puli możliwych do konfiguracji zasobów przetwarzania (np. sieci, serwerów, przestrzeni przechowywania, aplikacji i usług), które można szybko dostarczyć i uwolnić przy minimalnym wysiłku zarządzania lub działań dostawcy usługi. [12] Poczta elektroniczna udostępniana w ramach chmury obliczeniowej działa w ramach tzw. usługi „oprogramowanie jako usługa" (SaaS), która zapewnia użytkownikom kompletne odległe środowisko oprogramowania. Decydując się na stosowanie tego typu środków przetwarzania danych, powinno wziąć się pod uwagę opinię

[11] Chmury Obliczeniowe - Ekspertyza Dyrekcji Generalnej ds. Polityki Wewnętrznej Unii Europejskiej http://www.europarl.europa.eu/RegData/etudes/etudes/jom/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf
[12] Definicja Krajowego Instytutu Norm i Technologii Stanów Zjednoczonych (NIST) http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

5/2012 Grupy Roboczej Art. 29 w sprawie przetwarzania danych w chmurze obliczeniowej (tzw. cloud computing) (WP 196).

Uwzględniając zalecenia zawarte w ww. opinii Grupy Roboczej Art. 29, należy mieć świadomość ewentualnych (potencjalnych) zagrożeń związanych z chmurą obliczeniową. Większość tych zagrożeń zalicza się do dwóch szerokich kategorii: **brak kontroli nad danymi** oraz **niewystarczających informacji dotyczących samej operacji przetwarzania** (brak przejrzystości).

Ponadto istotne jest, aby korzystając z chmury obliczeniowej, posiadać pełne informacje o wszystkich fizycznych lokalizacjach serwerów, na których są lub mogą być przetwarzane dane osobowe.

IV. Podsumowanie wyników kontroli

1. Ogólna ocena kontrolowanej działalności

Czynności kontrolne przeprowadzone w kancelariach prawnych wykazały w zakresie objętym kontrolą nieprawidłowości w procesie przetwarzania danych osobowych, które polegały na nieodpowiednim zabezpieczeniu danych, braku niezbędnych elementów dokumentacji przetwarzania danych, a także na niezawarciu stosownych umów z podmiotami, którym powierzono przetwarzanie danych osobowych. Jednakże większość skontrolowanych podmiotów podjęła skuteczne działania mające na celu przywrócenie stanu zgodnego z prawem. Wyeliminowanie uchybień stwierdzonych w toku przeprowadzonych kontroli doprowadziło do sytuacji, w której w przeważającej liczbie skontrolowanych kancelarii zabezpieczenie danych osobowych jest obecnie prawidłowe.

2. Synteza wyników kontroli dokonana przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych.

Kontrole przeprowadzone w kancelariach prawnych wykazały, iż osiem (8) z dziesięciu skontrolowanych kancelarii naruszyło przepisy ustawy o ochronie danych. Stwierdzone w toku kontroli uchybienia polegały na:

1) niezabezpieczeniu danych osobowych przesyłanych w plikach w formacie DOC i PDF za pośrednictwem skrzynki poczty elektronicznej przed ich udostępnieniem osobom nieupoważnionym; pliki nie były zabezpieczone przed otwarciem (art. 36. ust. 1 ustawy[13]) – w jednym (1) podmiocie;

[13] **Art. 36 ust. 1 ustawy o ochronie danych osobowych.** Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2) niezawarciu w polityce bezpieczeństwa informacji o podmiotach, na serwerach których utrzymywana jest poczta elektroniczna oraz o podmiocie, na serwerach którego są zlokalizowane dane przetwarzane w aplikacji (§ 4 pkt 1 rozporządzenia[14]) - w pięciu (5) podmiotach;

3) niezawarciu w polityce bezpieczeństwa informacji o podmiocie, który serwisuje system informatyczny (§ 4 pkt 1 rozporządzenia) - w jednym (1) podmiocie;

4) niezawarciu w polityce bezpieczeństwa opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 3 i pkt 4 rozporządzenia[15]) – w czterech (4) podmiotach);

5) nietworzeniu kopii zapasowych plików zawierających dane osobowe, które są przetwarzane na komputerach użytkowanych w kancelarii (część A, pkt IV, ppkt 3 załącznika do rozporządzenia[16]) - w jednym (1) podmiocie;

6) niezawarciu z podmiotem, na serwerach którego utrzymywana jest poczta elektroniczna kancelarii, umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ustawy o ochronie danych osobowych[17] – w jednym (1) podmiocie;

7) niezawarciu z podmiotem serwisującym system informatyczny umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ustawy o ochronie danych osobowych – w jednym (1) podmiocie;

8) niezabezpieczeniu dysku sieciowego zawierającego dane osobowe klientów kancelarii przed dostępem osób nieupoważnionych oraz przed zabraniem przez osobę nieuprawnioną - dysk sieciowy znajdował się w niezamykanej na klucz szafie ustawionej w korytarzu, w którym przebywają osoby postronne (art. 36 ust. 1 ustawy) - w jednym (1) podmiocie.

V. Postępowanie kontrolne i działania podjęte po zakończeniu kontroli

Na podstawie dokonanych ustaleń, należy stwierdzić, że uchybienia, w szczególności dotyczące dokumentacji przetwarzania danych osobowych oraz bezpieczeństwa danych osobowych zostały niezwłocznie usunięte przez większość skontrolowanych kancelarii i wobec tego nie wszczęto wobec tych podmiotów postępowania administracyjnego.

---

14 § 4 pkt 1 rozporządzenia. Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

15 § 4 pkt 3 rozporządzenia. Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

16 **Część A, pkt IV, ppkt 3 załącznika do rozporządzenia.** Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

Natomiast wobec kancelarii prawnych, w których stwierdzono naruszenie przepisów o ochronie danych osobowych (wskazane w części IV pkt 1, 4, 5 i 6), wszczęte zostały postępowania administracyjne w celu przewrócenia stanu zgodnego z prawem.

Złączniki:

Wykaz aktów prawnych dotyczących przeprowadzonych kontroli.

Wykaz aktów prawnych dotyczących kontroli

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922).
2. Rozporządzenie 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 (Dz. U. Nr 100, poz. 1024).
3. Ustawa z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. z 2015 r. poz. 615) oraz wydane przez Naczelną Radę Adwokacką, na podstawie art. 3 ust. 1 pkt 5 tej ustawy, akty „korporacyjne", tj.:

   - Regulamin wykonywania zawodu adwokata w kancelarii indywidualnej lub spółkach będący załącznikiem do obwieszczenia Prezydium Rady Adwokackiej z dnia 7 lipca 2015 r. w sprawie ogłoszenia jednolitego tekstu Regulaminu wykonywania zawodu adwokata w kancelarii indywidualnej lub spółkach,

   - Zbiór Zasad Etyki i Godności Zawodu (Kodeks Etyki Adwokackiej) będący załącznikiem do obwieszczenia Prezydium Naczelnej Rady Adwokackiej z dnia 14 grudnia 2011 r. w sprawie ogłoszenia jednolitego tekstu Zbioru Zasad Etyki Adwokackiej i Godności Zawodu (Kodeks Etyki Adwokackiej),

   - Regulamin prowadzenia kont poczty elektronicznej w domenie adwokatura.pl. będący załącznikiem do obwieszczenia Prezydium Rady Adwokackiej z dnia 29 października 2013 r. w sprawie ogłoszenia jednolitego tekstu Regulaminu prowadzenia kont poczty elektronicznej w domenie adwokatura.pl.
4. Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (Dz. U. z 2016 r., poz. 233) oraz wydany przez Nadzwyczajny Krajowy Zjazd Radców Prawnych, na podstawie art. 57 tej ustawy Kodeks Etyki Radcy Prawnego będący załącznikiem do uchwały nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z dnia 22 listopada 2014 r. w sprawie Kodeksu Etyki Radcy Prawnego.