

Katalog Praw Przedsiębiorców

**Generalny Inspektor Ochrony
Danych Osobowych**

ZESZYT 3.

Opracowanie: Kancelaria JWMS Jakubowski Wiese Mazgaj Staszek radcowie prawni



O KANCELARII



Kancelaria JWMS Jakubowski Wiese Mazgaj Staszek radcowie prawni powstała jako wspólne przedsięwzięcie czterech radców prawnych, którzy doświadczenie zawodowe zdobyte w czołowych krakowskich kancelariach i w organach administracji publicznej oraz karierę akademicką na Uniwersytecie Jagiellońskim łączą z praktyczną znajomością biznesu.

SPECJALIZACJA

Kancelaria JWMS oferuje świadczenie kompleksowych usług prawnych – zarówno dla dużych przedsiębiorstw, jak i dla podmiotów z sektora MSP. Dzięki dużej różnorodności specjalizacji wspólników JWMS, Kancelaria zapewnia najwyższą jakość w obsłudze prawnej przedsiębiorstw z wielu branż, świadcząc usługi w obrębie szerokiego spektrum dziedzin prawa. Praktyka Kancelarii JWMS koncentruje się przede wszystkim na zagadnieniach z obszaru prawa gospodarczego (w tym prawa spółek), prawa cywilnego (ze szczególnym uwzględnieniem prawa umów), prawa pracy oraz prawa administracyjnego.

Oferta Kancelarii JWMS skierowana jest nie tylko do przedsiębiorstw działających w kraju, ale również do podmiotów operujących na rynkach zagranicznych. Zarówno do przedsiębiorstw z wieloletnią tradycją, jak i do innowacyjnych, pionierskich przedsięwzięć.

Więcej informacji na stronie:

<http://jwms.pl/>

WSTĘP

Niniejsze opracowanie ma na celu przybliżenie przedsiębiorcom procedury kontroli w zakresie zgodności z prawem przetwarzania danych osobowych. Kontrolę taką sprawuje Generalny Inspektor Ochrony Danych Osobowych, z reguły za pośrednictwem pracowników swojego Biura, zwanych inspektorami.

Kontrole są prowadzone pod kątem zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa, głównie zaś z ustawą o ochronie danych osobowych. Przedsiębiorca jest zobowiązany do przestrzegania szeregu obowiązków wskazanych przez przepisy prawa. Przede wszystkim jest zaś zobowiązany do zapewnienia bezpieczeństwa przetwarzania danych osobowych, w szczególności natomiast jego obowiązkiem jest prowadzenie dokumentacji dotyczącej podjętych środków. Najważniejsze z nich to Polityka Bezpieczeństwa Informacji i Instrukcja Zarządzania Systemem Informatycznym.

Co do zasady, kontrole są zapowiadane. Od momentu zawiadomienia, do momentu przeprowadzenia kontroli musi upłynąć minimalnie 7, a maksymalnie 30 dni. Po upływie tego czasu konieczne jest nowe zawiadomienie. Kontrole nie mogą się kumulować. Jeśli zatem w danym czasie u przedsiębiorcy przeprowadzana jest kontrola przez organ inny niż GIODO, przedsiębiorca ma prawo żądać od niego zaprzestania kontroli i wyznaczenia innego terminu. Ponadto ograniczony jest również okres, w jakim mogą trwać w sumie wszystkie kontrole w danym roku kalendarzowym. Wynosi on od 12 (w przypadku mikroprzedsiębiorców) do 48 dni (w przypadku przedsiębiorców spoza sektora MŚP).

Kontrolę z reguły przeprowadzają inspektorzy – pracownicy Biura GIODO. Mają oni szerokie uprawnienia, warto jednak pamiętać, że przedsiębiorca ma prawo zażądać przedłożenia mu legitymacji służbowej i upoważnienia wydanego przez GIODO.

Po zakończonej kontroli inspektor jest zobowiązany do sporządzenia protokołu, który powinien być podpisany przez przedsiębiorcę. Przed-

siębiorca może zgłosić do protokołu umotywowane uwagi i zastrzeżenia. Ma ponadto prawo do wniesienia do GIODO umotywowanego sprzeciwu wobec przeprowadzenia kontroli w terminie 3 dni od jej wszczęcia. Sprzeciw taki powoduje wstrzymanie czynności kontrolnych.

W wypadku stwierdzenia naruszeń, inspektorzy przekazują sprawę do GIODO, który może zastosować środki administracyjne. Ponadto zawiadamia on organy powołane do ścigania przestępstw, jeżeli wskutek kontroli doszło do ujawnienia okoliczności, które wskazują na popełnienie przez przedsiębiorcę (będącego administratorem danych osobowych) przestępstwa w związku z przetwarzaniem przez niego danych osobowych.

KONTROLA PODMIOTÓW PRZETWARZAJĄCYCH DANE OSOBOWE

Kontrolę przedsiębiorców przetwarzających dane osobowe przewiduje ustawa o ochronie danych osobowych z 29 sierpnia 1997 roku (tekst jedn.: Dz.U. z 2002 roku, nr 101, poz. 926 z późn. zm.). Stosuje się ją do wszystkich osób fizycznych i osób prawnych oraz do jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych. Dotyczy to przede wszystkim przedsiębiorców, którzy w ramach swojej działalności gospodarczej przetwarzają dane osobowe, czyli pełnią funkcję tzw. administratora danych osobowych.

Wspomniana ustawa wskazuje, że przetwarzanie danych osobowych to ich zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie lub usuwanie. W dzisiejszych czasach dotyczy to głównie operacji dokonywanych na danych osobowych w systemach informatycznych – począwszy od skomplikowanych sieci wewnętrznych, a na *smartfonach* skończywszy.

Niemal każdy przedsiębiorca w ramach swej działalności przetwarza dane osobowe. Są to m.in. dane klientów, kontrahentów, usługobiorców, czy wreszcie pracowników.

Do kontroli, o której mowa, powołany jest Generalny Inspektor Ochrony Danych Osobowych (w skrócie: GIODO). Powierzone mu przez ustawę zadania kontrolne wykonuje on samodzielnie lub za pośrednictwem swojego zastępcy (Zastępcy Generalnego Inspektora), a w większości przypadków za pośrednictwem znacznej liczby inspektorów, czyli upoważnionych przez niego pracowników Biura GIODO.

ZAKRES KONTROLI

Kontrolę przeprowadza się w zakresie zgodności przetwarzania danych osobowych z przepisami o ich ochronie. Warto podkreślić, że kontrola jest sprawowana bez względu na to, w jakiej formie dochodzi do przetwarzania danych osobowych, a zatem nawet, gdy odbywa się to poza zbiorami danych (czyli nie dotyczy ona rzadko używanych teczek, przechowywanych w archiwum lub szafie, ale wszelkich danych osobowych, którymi kontrolowany podmiot dysponuje, np. imion i nazwisk klientów sklepu internetowego, które nie są fizycznie przechowywane i grupowane według jakichkolwiek kluczy). Ponadto kontrola nie ogranicza się do zgodności z przepisami ustawy o ochronie danych osobowych, ale rozciąga się na wszystkie przepisy, które obowiązują na terenie RP i dotyczą tej ochrony (w tym inne ustawy czy rozporządzenia). Przykładowo można wskazać na rozporządzenie Ministra Spraw Wewnętrznych i Administracji 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. z 2004 roku, nr 100, poz. 1024), w którym reguluje się, między innymi, zasady tworzenia dokumentacji przetwarzania danych osobowych.

OBOWIĄZKI PRZEDSIĘBIORCY PRZETWARZAJĄCEGO DANE OSOBOWE

Aby uchronić się przed negatywnymi konsekwencjami kontroli Generalnego Inspektora Ochrony Danych Osobowych, należy wypełniać obowiązki, jakie spoczywają na przedsiębiorcy, który jest administratorem danych osobowych. Najważniejsze z nich zostaną opisane poniżej.

Pierwszym i najważniejszym obowiązkiem przedsiębiorcy przetwarzającego dane osobowe w zbiorze danych jest dokonanie zgłoszenia zbioru danych do rejestru prowadzonego przez GIODO. Jedyne wyjątki od tego obowiązku są wskazane w art. 43 ustawy o ochronie danych osobowych. Przykładem może być brak obowiązku zgłoszenia danych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej. Zgłoszenie powinno wskazywać m.in. adres siedziby administratora, cel przetwarzania danych osobowych oraz sposób zbierania i udostępniania danych. Administrator danych musi także zgłaszać GIODO każdą zmianę tego typu informacji w terminie do 30 dni od jej dokonania, czyli np. jest zobowiązany poinformować GIODO o zmianie sposobu zbierania danych.

Wskazanie w zgłoszeniu celu przetwarzania danych osobowych ma bardzo duże znaczenie od strony praktycznej. Dane osobowe mogą być bowiem przetwarzane tylko w celu, na jaki uzyskało się zgodę od osoby, której dotyczą. Każde jego przekroczenie jest naruszeniem przepisów.

Na przedsiębiorcy ciąży obowiązek zapewnienia ochrony przetwarzanych danych osobowych. Jest on zobowiązany do wdrożenia środków technicznych i organizacyjnych, które pozwolą uniknąć takich zagrożeń, jak dostęp do danych osoby nieuprawnionej, czy uszkodzenie lub utrata danych. Środkami takimi są np. ustalenie hasła dostępu do zbioru danych, odpowiednie ustawienie monitorów w pomieszczeniu, czy wreszcie zastosowanie systemów antywłamaniowych. Środki powinny być proporcjonalne do zagrożeń i kategorii danych. Stąd też bardziej zaawansowane metody należy stosować do chronienia tzw. danych wrażliwych, takich jak pochodzenie etniczne, czy przynależność wyznaniowa.

Jednym z wymogów, mających na celu zabezpieczenie przetwarzanych danych osobowych, jest prowadzenie dokumentacji zastosowanych środków. Składają się na nią Polityka Bezpieczeństwa Informacji i Instrukcja Zarządzania Systemem Informatycznym. Dokumenty te muszą zostać sporządzone w formie pisemnej. Powinny w sposób szczegółowy opisywać zarówno fizyczną, jak i informatyczną infrastrukturę, w której przetwarzane są dane osobowe. Odpowiednie sporządzenie tych dokumentów może powodować pewne trudności, gdyż wymogi dotyczące ich przygotowania określone w rozporządzeniu ministra są bardzo szczegółowe. W razie kontroli przedsiębiorca jest zobowiązany do zapewnienia inspektorowi dostępu do tych dokumentów.

W zakresie zapewnienia ochrony danych osobowych administrator danych ma obowiązek kontrolować kto, kiedy i jakie dane wprowadza do zbioru oraz komu są one przekazywane, powinien ponadto prowadzić ewidencję osób upoważnionych do ich przetwarzania.

Współcześnie coraz powszechniejsze staje się powierzenie danych osobowych do przetwarzania innym podmiotom. Przedsiębiorca ma do tego prawo, ale musi w tym celu zawrzeć stosowną umowę, przewidzianą w ustawie o ochronie danych osobowych. Podmiot, któremu powierza się przetwarzanie danych osobowych, musi spełniać wymogi określone przez tę ustawę, takie jak np. zapewnienie określonych środków techniczno-organizacyjnych. Niemniej jednak, w wypadku naruszenia danych przez ów podmiot, odpowiedzialność będzie spoczywać na przedsiębiorcy powierzającym podmiotowi przetwarzanie danych.

Na przedsiębiorcy ciążyą także obowiązki informacyjne w stosunku do osoby, której dane mają być przetwarzane. Musi ona zostać poinformowana m.in. o adresie i pełnej nazwie administratora danych, celu ich przetwarzania, prawie dostępu do nich i dobrowolności lub obowiązku ich podania. W wypadku, gdy dane pochodzą od podmiotu innego niż zainteresowana osoba, należy ją także pouczyć o zakresie przetwarzanych danych, możliwości ich poprawienia, zażądania zaprzestania ich przetwarzania i możliwości wniesienia sprzeciwu. Ponadto trzeba podać źródło, z jakiego dane pochodzą. Na wniosek osoby, której dane dotyczą, administrator danych jest zobowiązany do udzielenia (w ciągu 30 dni) informacji dotyczących zbioru,

w którym dane tej osoby są przetwarzane. W razie wykazania przez osobę, której dane dotyczą, że dane są niekompletne, nieaktualne lub nieprawdziwe, administrator jest zobowiązany do uzupełniania, uaktualniania i prostowania danych.

Jeśli przedsiębiorca świadczy usługi drogą elektroniczną, musi pamiętać m.in. o tym, aby zakończyć przetwarzanie danych osobowych zaraz po skończeniu korzystania z usługi przez usługobiorcę. Będzie mógł je jednak przetwarzać w celach reklamowych lub badań rynku w przypadku, gdy osoba, której dane dotyczą, wyrazi na to zgodę i przetwarzanie będzie służyło poprawieniu jakości świadczenia usług.

Dopełnienie wyżej opisanych obowiązków jest niezwykle istotne. Oprócz środków administracyjnych, które może zastosować GIODO, przedsiębiorca jest także zagrożony sankcjami karnymi, które wiążą się ze złamaniem przepisów o ochronie danych osobowych. Najostrzejsza sankcja przewidziana jest w wypadku przetwarzania tzw. wrażliwych danych osobowych, których przetwarzanie jest niedopuszczalne lub do którego przetwarzania przedsiębiorca nie ma uprawnienia. Może ona wynieść nawet 3 lata pozbawienia wolności. Jeśli takie naruszenie dotyczy innych danych, sankcja wynosić może 2 lata więzienia. Warto wspomnieć, że nawet nieumyślne udostępnienie danych osobom nieuprawnionym jest zagrożone karą do roku pozbawienia wolności. Taka sankcja jest przewidziana również w wypadku niedopełnienia innych obowiązków opisanych powyżej, np. jeśli nie zostanie zgłoszony zbiór do rejestru, czy nie dojdzie do zabezpieczenia danych przed uszkodzeniem. Przedsiębiorcy muszą zatem bardzo uważnie pilnować wszystkich obowiązków nałożonych na nich w ramach przepisów.

NAJCZĘSTSZE BŁĘDY PRZEDSIĘBIORCÓW

Przedsiębiorcy przetwarzający dane osobowe popełniają kilka podstawowych błędów, które mogą prowadzić do bardzo przykrych konsekwencji, takich jak sankcje administracyjne (zakaz przetwarzania danych, obowiązek usunięcia danych), czy nawet karne (za przetwarzanie danych osobowych bez uprawnienia grożą nawet 3 lata pozbawienia wolności).

Pierwszym podstawowym błędem jest brak zgłoszenia zbioru danych do rejestru prowadzonego przez GIODO. Zgłoszenie takie może być dokonane internetowo, za pomocą udostępnionego przez GIODO interaktywnego formularza. Zgłoszenie uznaje się za dokonane z chwilą jego wystania (a nie zatwierdzenia rejestracji przez GIODO), a poziom trudności wypełnienia formularza podobny jest do poziomu trudności wypełnienia zeznania PIT. Zgłoszenia dokonuje się raz na zawsze, w związku z czym tym większy żal do siebie mają ci, którzy zaniedbają ten obowiązek.

Drugim błędem popełnianym przez przedsiębiorców jest brak dokumentacji przetwarzania danych osobowych. Dokumentacja ta powinna składać się z Polityki Bezpieczeństwa Informacji oraz z Instrukcji Zarządzania Systemem Informatycznym. Dokumentacja jest bardzo obszerna (zwykle liczy ok. 30 stron) i powinna zostać przygotowana przez profesjonalnego prawnika. Względnie wysoki koszt usługi częściowo wyjaśnia fakt braku ww. dokumentów, ale GIODO nie przewiduje ulg nawet dla najuboższych administratorów danych osobowych.

Trzecim błędem jest używanie danych osobowych w celach, na które przedsiębiorcy nie mają zgody osoby, której dane dotyczą. Na przykład: nie wolno wykorzystywać do celów marketingowych danych osobowych kontrahentów, które zamieszczono w fakturach i umowach (ponieważ dane te można przetwarzać jedynie w celu wykonania umowy, chyba że kontrahent wyraźnie zgodził się na wykorzystanie ich w celach marketingowych). Lepiej więc nie wysyłać klientom z okazji Bożego Narodzenia kartek z życzeniami, na których wykorzystane zostały dane z faktur.

Czwartym błędem, szczególnie groźnym, jest powierzanie danych osobowych podmiotom trzecim bez zawarcia umowy o powierzeniu danych osobowych do przetwarzania. Jest to o tyle ryzykowne, że taka umowa ma na celu właśnie ochronę interesów przedsiębiorcy, który powierza dane osobowe jakimi administruje, np. zewnętrznemu handlowcowi. Jeśli bowiem handlowiec ten będzie przetwarzał powierzone mu dane niezgodnie z prawem (np. sprzeda dane innemu przedsiębiorcy lub sam wykorzysta je do własnych celów), to za wszystkie naruszenia ustawy odpowie administrator danych, który powierzył je handlowcowi. Umowa o powierzeniu danych osobowych do przetwarzania nie zwalnia z tej odpowiedzialności administratora, ale pozwala mu, w razie potrzeby, dochodzić od osoby, której powierzył dane, odszkodowania lub kary umownej.

Reszta zaniedbań, dokonywanych przez przetwarzających dane osobowe, dotyczy raczej kwestii techniczno-organizacyjnych. Na przykład sprzęt komputerowy, za pomocą którego można uzyskać dostęp do danych osobowych (w tym również *smartfony*), nie jest zabezpieczony hasłem lub w biurze, gdzie przechowywane są dane w postaci wydruków (albo znajduje się serwer), nie ma gaśnicy czy drzwi antywłamaniowych. Szereg wymagań w zakresie zabezpieczeń fizycznych i zabezpieczeń systemu informatycznego wynika ze stosownych rozporządzeń.

Powyżej opisane błędy nachodzą na siebie i mogą się kumulować lub nawet mnożyć. Przykładowo, jeśli przedsiębiorca nie ma dokumentacji przetwarzania danych osobowych (jest to pierwsza rzecz, o którą pyta kontrola z GIODO), to teoretycznie nie powinien dokonywać zgłoszenia zbioru danych osobowych do rejestru GIODO. Wynika to z tego, że podczas zgłaszania formularza danych konieczne jest zaznaczenie odpowiedniego *checkboxa*, przez co potwierdza się posiadanie dokumentacji. Jak można się domyślić, przedsiębiorcy przez nieuwagę lub z innych względów niekiedy zaznaczają feralny *checkbox*, pomimo że nie posiadają Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym. Dochodzi więc do poświadczenia nieprawdy, które jest poważnym przestępstwem.

PROCEDURA KONTROLI

Procedura kontroli przedsiębiorcy – administratora danych – musi spełniać wymogi ustawy o ochronie danych osobowych, a ponadto być zgodna z postanowieniami ustawy o swobodzie działalności gospodarczej (tekst jedn.: Dz.U. z 2013 roku, poz. 672 z późn. zm.).

Przedsiębiorca powinien być powiadomiony o zamiarze przeprowadzenia kontroli. Od zawiadomienia do wszczęcia kontroli musi upłynąć 7 dni, jednak nie więcej niż 30. W razie upływu terminu kolejna kontrola może być wszczęta jedynie po ponownym zawiadomieniu. Zawiadomienie powinno zawierać m.in. wskazanie zakresu przedmiotowego kontroli.

Jak zostało wspomniane, do przeprowadzenia kontroli uprawnieni są, obok Generalnego Inspektora i jego Zastępcy, pracownicy Biura GODO, którzy posiadają upoważnienie, czyli inspektorzy.

Przed rozpoczęciem kontroli przedsiębiorca ma prawo żądać przedłożenia mu legitymacji służbowej oraz upoważnienia do przeprowadzenia kontroli. Upoważnienie nie obejmuje zlecenia przeprowadzenia ekspertyz lub sporządzenia opinii.

Inspektor powinien ponadto poinformować przedsiębiorcę lub inną osobę, wobec której podejmuje czynności kontrolne, o jego prawach i obowiązkach w trakcie kontroli. Pouczenie takie zazwyczaj ma formę pisemną i jest zawarte w dokumentach przedstawianych przedsiębiorcy.

Kontrolę przeprowadza się w obecności kontrolowanego lub osoby przez niego upoważnionej na piśmie. Kontrola powinna być przeprowadzona w czasie faktycznego wykonywania działalności gospodarczej przez kontrolowanego. Ustawa o ochronie danych osobowych daje jednak kontrolerom możliwość wstępu do pomieszczeń w godzinach 6.00-22.00. Wymaga się, aby kontrola była zawsze przeprowadzana w sposób sprawny i możliwie niezakłócający funkcjonowania przedsiębiorstwa.

Zgodnie z ustawą o swobodzie działalności gospodarczej nie można podejmować i prowadzić więcej niż jednej kontroli równocześnie. Przedsiębiorca ma zatem prawo żądać od inspektorów GIODO rezygnacji z przeprowadzenia kontroli i wyznaczenia innego terminu, jeśli w tym samym czasie prowadzona jest już wobec niego kontrola innego organu.

Przedsiębiorca przed rozpoczęciem kontroli powinien zostać poinformowany o planowanym terminie jej zakończenia. Jednocześnie ustawa wyznacza również czas wszystkich kontroli przeprowadzanych przez GIODO w roku kalendarzowym. Kontrole mogą trwać w sumie:

- w odniesieniu do mikroprzedsiębiorców – 12 dni roboczych,
- w odniesieniu do małych przedsiębiorców – 18 dni roboczych,
- w odniesieniu do średnich przedsiębiorców – 24 dni roboczych,
- w odniesieniu do pozostałych przedsiębiorców – 48 dni roboczych.

Jeżeli wyniki przeprowadzonej kontroli wykazały rażące naruszenie przepisów o ochronie danych osobowych, dopuszczalne jest przeprowadzenie powtórnej kontroli w tym samym zakresie w danym roku kalendarzowym, nawet jeśli zostanie przekroczony limit czasowy wskazany powyżej. Czas trwania powtórnej kontroli nie może jednak przekroczyć 7 dni.

Przedsiębiorca jest zobowiązany do prowadzenia książki kontroli (może ona mieć formę elektroniczną), która służy do dokumentowania czasu trwania i liczby kontroli jego działalności. Dokument ten jest udostępniany inspektorowi w toku dokonywanej kontroli.

Wszystkie powyżej opisane procedury są obowiązującymi zasadami. W niektórych przypadkach dopuszczalne jest jednak odstępnie od zawiadomienia o kontroli, przeprowadzenie jej bez udziału przedsiębiorcy lub osoby przez niego upoważnionej, a także równoległe do innej kontroli. Ponadto możliwe jest przekroczenie rocznych limitów czasowych. Wyjątki te dotyczą sytuacji:

- kontroli prowadzonej w celu przeciwdziałania popełnieniu przestępstwa lub wykroczenia, przeciwdziałania popełnieniu przestępstwa skarbowego lub wykroczenia skarbowego, a także zabezpieczenia dowodów jego popełnienia,

– przeprowadzenia kontroli, które uzasadnione jest bezpośrednim zagrożeniem życia, zdrowia lub środowiska naturalnego.

UPRAWNIENIA INSPEKTORA

Najważniejszym uprawnieniem inspektora jest wstęp do pomieszczenia, w którym znajduje się zbiór danych osobowych lub, jeśli dane są przetwarzane poza zbiorem, do pomieszczenia, w którym się to odbywa. W pomieszczeniach tych może dokonywać wszystkich badań i czynności, które są konieczne w celu zweryfikowania zgodności z prawem przetwarzania danych osobowych.

Inspektor ma także wgląd do wszystkich dokumentów i danych, które mają związek z kontrolowanym aktualnie przetwarzaniem danych. Może także sporządzać kopie owych dokumentów. W ramach kontroli inspektorzy dokonują również oględzin urządzeń, nośników i systemów informatycznych.

Co ważne, inspektor uprawniony jest do zażądania od administratora przedstawienia ustnych lub pisemnych wyjaśnień, a także do przesłuchiwania innych osób.

Kontrola przetwarzania danych osobowych wymaga niejednokrotnie dużej wiedzy specjalistycznej, stąd też inspektorom zostało przyznane uprawnienie do zlecenia wykonania opinii i ekspertyz specjalistom (np. z zakresu informatyki).

Wszystkie uprawnienia inspektorzy mogą wykorzystywać jedynie w takim zakresie, w jakim odnoszą się one do przeprowadzanej kontroli i jej przedmiotu.

Umożliwienie inspektorowi wykonania opisanych czynności jest obowiązkiem kierownika jednostki organizacyjnej, w której przetwarzane są dane osobowe lub która jest administratorem danych, bądź też obowiązkiem administratora danych osobowych, jeśli jest osobą fizyczną. Udaremnianie lub utrudnianie wykonywania czynności kontrolnych jest zagrożone sankcją karną wynoszącą nawet do 2 lat pozbawienia wolności.

PO KONTROLI

Inspektor jest zobowiązany do sporządzenia protokołu ze wszystkich przeprowadzonych przez siebie czynności. Protokół taki musi być podpisany przez niego, a także przez kontrolowanego administratora danych, który może wnieść do protokołu umotywowane uwagi i zastrzeżenia.

Uprawnienia inspektorów ograniczają się w zasadzie jedynie do przeprowadzenia kontroli. Po zakończonej kontroli, jeśli jej wyniki tego wymagają, mogą oni jedynie żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym uchybień. Mogą zażądać również poinformowania w określonym terminie o wynikach postępowania i podjętych działaniach.

Jeżeli na podstawie wyników kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do GIODO o zastosowanie wskazanych w ustawie środków, które mają na celu przywrócenie zgodnego z prawem stanu. Są to przede wszystkim środki wymienione w ustawie o ochronie danych osobowych, czyli:

- usunięcie uchybień,
- uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,
- zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,
- wstrzymanie przekazywania danych osobowych do państwa trzeciego,
- zabezpieczenie danych lub przekazanie ich innym podmiotom,
- usunięcie danych osobowych.

W sprawie zastosowania tych środków GIODO wydaje decyzję administracyjną. Ich wykonanie jest obowiązkiem przedsiębiorcy, który pełni funkcję administratora danych, ewentualnie podmiotu, który przetwarza dane na jego zlecenie.

Warto wskazać, że wydanie takiej decyzji może nastąpić na wniosek osoby zainteresowanej. Osobą zainteresowaną jest przede wszystkim osoba, której dane są przetwarzane. Może ona wnioskować bezpośrednio do GIODO o wydanie określonej decyzji. Wtedy wydanie decyzji nie musi (ale może) być poprzedzone opisaną wyżej kontrolą.

Wydanie decyzji w każdym wypadku poprzedzone jest jednak postępowaniem administracyjnym, w ramach którego można dokonać kontroli przedsiębiorcy przetwarzającego dane. Wszystkie wyżej wymienione uwagi mają zastosowanie także w przypadku takiej kontroli. W takim postępowaniu przedsiębiorca zyskuje uprawnienia strony postępowania administracyjnego.

GIODO zawiadamia organy powołane do ścigania przestępstw, jeśli stwierdzi, że działania podejmowane w związku z przetwarzaniem danych osobowych noszą znamiona przestępstwa. Dotyczy to:

- przetwarzania danych przez osoby nieuprawnione,
- udostępniania danych osobom nieuprawnionym,
- naruszenia obowiązku zabezpieczenia danych,
- niezgłoszenia danych do rejestru,
- niedopełnienia obowiązku poinformowania,
- udaremnienia wykonania czynności kontrolnej.

UPRAWNIENIA PRZEDSIĘBIORCY

Ustawa o ochronie danych osobowych przewiduje, że kontrolowany przedsiębiorca, będący administratorem danych, może wnosić umotywowane zastrzeżenia i uwagi do protokołu.

Pozostałe uprawnienia przedsiębiorcy – administratora danych – wskazane są w ustawie o swobodzie działalności gospodarczej.

Ważnym uprawnieniem kontrolowanego przedsiębiorcy jest możliwość wniesienia sprzeciwu. Sprzeciw może dotyczyć podjęcia lub wykonywania

czynności z naruszeniem przepisów. Sprzeciw wnosi się na piśmie do organu podejmującego i wykonującego kontrolę (a zatem do GIODO, nie do inspektora) w terminie do 3 dni roboczych od dnia wszczęcia kontroli. Musi on być uzasadniony. Sprzeciw powoduje wstrzymanie czynności kontrolnych oraz wstrzymanie czasu przeznaczanego na kontrolę, aż do momentu rozpatrzenia sprzeciwu. Następnie, w zależności od postanowienia GIODO, kontrola nie jest przeprowadzana lub jest kontynuowana.

Jeśli w wyniku kontroli przeprowadzonej z naruszeniem prawa przedsiębiorca poniesie szkodę, ma on prawo żądać odszkodowania na zasadach ogólnych, przewidzianych w Kodeksie cywilnym. W reakcji na decyzje administracyjne wydawane przez GIODO adresat decyzji (strona) ma prawo zwrócić się do GIODO z wnioskiem o ponowne rozpatrzenie sprawy. Z kolei na decyzję w przedmiocie tego wniosku można wnieść skargę do sądu administracyjnego.

PODSTAWA PRAWNA:

- ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2002 roku, nr 101, poz. 926 ze zm.),
- ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (tekst jedn.: Dz.U. z 2013 roku, poz. 672 ze zm.),
- ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (tekst jedn.: Dz.U. z 2013 roku, poz. 267 ze zm.),
- ustawa z dnia 19 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (tekst jedn.: Dz.U. z 2012 roku, poz. 1015 ze zm.),
- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. z 2004 roku, nr 100, poz. 1024).

Związek Przedsiębiorców i Pracodawców | www.zpp.net.pl

Kancelaria JWMS Jakubowski Wiese Mazgaj Staszek radcowie prawni | www.jwms.pl

Wydawnictwo WEI

© Copyright by Związek Przedsiębiorców i Pracodawców, Warszawa 2014