

Biura rachunkowe są wciąż na celowniku GIODO

Firmy notorycznie nie podpisują z klientami umów o **powierzenie przetwarzania danych osobowych** i stają się przez to ich administratorami. Działają więc ze szkodą dla siebie

Jakub Styczyński
jakub.styczynski@infor.pl

Wiele firm uważa, że ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (dalej: u.o.o.d.o.) nie dotyczy biur rachunkowych, ponieważ nie istnieją przepisy wprost nakładające na nie zadania z zakresu ochrony informacji. Rzecz w tym, że specyfika branży biur rachunkowych sprawia, iż dane osobowe przez nie przetwarzane mogą być uważane za informacje poufne. Ponadto biura często nie wiedzą o konieczności podpisania stosownej umowy powierzenia danych przez klienta ani że wykonują czynności, które mogą stawiać ich w roli administratora danych – tym samym tworząc obowiązek ich zabezpieczenia. Generalny inspektor ochrony danych osobowych (GIODO) ostrzega, że brak spełnienia wymogów przez biura rachunkowe może skutkować dotkliwymi sankcjami.

– W ostatnich latach przeprowadzaliśmy wiele kontroli w biurach rachunkowych i okazało się, że najwięcej problemów mają one z prawidłowym wykonaniem podstawowych obowiązków wynikających z przepisów o ochronie danych osobowych – informuje Małgorzata Kałużyńska-Jasak, dyrektor zespołu rzecznika prasowego GIODO. I dodaje, że uchybienia w tym zakresie dotyczyły w szczególności niezgłoszenia do rejestracji GIODO prowadzonych zbiorów danych osobowych, dopuszczenia do przetwarzania danych osób nieposiadających upoważnień nadanych przez administratora danych, braków ewidencji osób upoważnionych do przetwarzania danych osobowych, polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Inspektor krytycznie ocenił również sposób wykonania obowiązków związanych z przetwarzaniem danych przy użyciu systemów informatycznych.

Kiedy obowiązkowo

Biura rachunkowe najczęściej nie są administratorami danych osobowych, tylko otrzymują je od swoich klientów. Należy jednak pamiętać, że zgodnie z art. 31 ust. 1 u.o.o.d.o. przekazanie informacji przez klienta (w tym przypadku administratora danych) powinno odbyć się w oparciu o umowę zawartą na piśmie (to tzw. umowa powierzenia przetwarzania danych osobowych). Według GIODO, który otrzymywał informacje od Państwowej Inspekcji Pracy, biura często zapominają o jej sporządzeniu. Umowa ta sprawia, że przekazujący dane po jej podpisaniu wciąż pozostaje administratorem danych. Biura rachunkowe nie muszą zatem zgłaszać bazy danych do GIODO, zwłaszcza że przepisy dodatkowo wyłączają je od tej odpowiedzialności. Zgodnie z art. 43 ust. 1 pkt 8 u.o.o.d.o. baz nie muszą ich bowiem zgłaszać podmioty, które wykorzystują dane wyłącznie w celu stworzenia dokumentów pracowniczych, pracy w oparciu o wyciągi bankowe, umowy czy faktury.

Należy jednak pamiętać, by umowa przetwarzania danych osobowych z klientem wyraźnie określała zakres i cel przetwarzania tych informacji, gdyż biura rachunkowe mogą je przetwarzać tylko w tych ramach. To ważne, bo firmy często wykraczają poza czynności uwzględnione w umowie tworząc własne zbiory informacji jak np. wewnętrzny rejestr przedsiębiorców powierzających dane. Jeśli te bazy danych tworzone najczęściej w celach rozliczeniowych mają być wykorzystywane także w innych celach, np. marketingowych,

dochodzenia roszczeń albo prowadzenia postępowań reklamacyjnych, to biura rachunkowe stają się wtedy samodzielnymi administratorami własnych zbiorów danych. Automatycznie ciąży na nich obowiązek nie tylko zgłoszenia tych baz do GIODO ale również podjęcia środków zabezpieczających informacje jeszcze przed wykonaniem jakichkolwiek czynności uwzględniających ich wykorzystanie..

Polityka bezpieczeństwa danych i instrukcja

Środki zabezpieczające informacje opisuje art. 39 ust. 1 u.o.o.d.o., a doprecyzowuje par. 4 i 5 rozporządzenia ministra spraw wewnętrznych i administracji z 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. Wymieniona w rozporządzeniu dokumentacja obejmuje politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. [ramka]

System informatyczny do przetwarzania danych osobowych powinien zapewniać określony poziom bezpieczeństwa – w zależności od rodzaju informacji, jakie magazynuje. Są trzy: podstawowy, podwyższony oraz wysoki. Przykładowo pierwszy stosuje się w systemach, które nie przetwarzają danych wrażliwych (np. o stanie zdrowia, skazaniu, mandatach, pochodzeniu rasowym lub etnicznym) oraz nie są połączone z publiczną siecią. Przy każdej osobie, której dane osobowe są przetwarzane w systemie informatycznym, należy odnotować datę pierwszego wprowadzenia danych do systemu oraz utworzyć identyfikator dla pracownika wprowadzającego dane osobowe do systemu. Ponadto należy zmieniać hasło dostępu do systemu częściej niż raz na 30 dni i stosować kryptograficzną ochronę informacji (tzn. powinny być one zaszyfrowane i przesyłane między stanowiskami w sposób niejawny).

Lista pracowników z dostępem do danych

Zgodnie z art. 36a u.o.o.d.o. przedsiębiorcy zajmujący się prowadzeniem biur rachunkowych mogą, ale nie muszą powoływać tzw. administratora bezpieczeństwa informacji (ABI). Zaletą płynącą z posiadania ABI jest zwolnienie z obowiązku rejestrowania zbiorów danych osobowych u GIODO. Osoba na tym stanowisku zajmuje się bowiem m.in. sprawdzaniem zgodności przetwarzania danych z przepisami u.o.o.d.o.

Biuro rachunkowe decydując się na powołanie ABI, zapewnia w takim przypadku większą ochronę danych powierzonych przez klientów. Warto to rozważyć, zwłaszcza że przepisy zastrzegają jedynie trzy podstawowe wymogi, jakie musi spełnić osoba brana pod uwagę na stanowisko ABI. Mianowicie kandydat musi mieć pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych, nie być karany za umyślne przestępstwo oraz mieć odpowiednią wiedzę w zakresie danych osobowych.

Jeśli chodzi o resztę pracowników, to każda osoba wykorzystująca w jakiś sposób dane osobowe w firmie (np. zbieranie ich, przechowywanie, przetwarzanie, wprowadzanie zmian bądź usuwanie ich) musi mieć ku temu odpowiednie upoważnienie. Biuro rachunkowe powinno przygotować listę pracowników upoważnionych, uwzględniając: imię i nazwisko tych osób, datę nadania i ustania oraz zakres upoważnienia do

Polityka bezpieczeństwa powinna zawierać w szczególności:

wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,

wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

sposób przepływu danych pomiędzy poszczególnymi systemami,

określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych powinna zawierać w szczególności:

procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,

stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,

procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników, – procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,

sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych,

sposób zabezpieczenia systemu informatycznego,

procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

pracy z danymi osobowymi oraz sporządzić identyfikatory dla tych, którzy korzystają z danych przetwarzanych w specjalnie przygotowanym systemie informatycznym.

Czego należy się bać

Przepisy przewidują odpowiedzialność zarówno administracyjną (art. 18 u.o.o.d.o.), jak i karną, szczegółowo uregulowaną przez art. 49–54a. GIODO może nakazać podmiotowi usunięcie uchybień, poprawę danych, zastosowanie dodatkowych środków zabezpieczających. W skrajnych przypadkach może samodzielnie zabezpieczyć dane, usunąć je lub przekazać innym podmiotom.

Inspektor ma również prawo nałożyć grzywnę na podmiot w przypadku niewykonania wydanej przez niego decyzji. Kwota grzywny może wynieść maksymalnie 10 tys. zł w stosunku do osoby fizycznej i maksymalnie 50 tys. zł w stosunku do osób prawnych. Jednocześnie grzywny nakładane wielokrotnie nie mogą łącznie przekroczyć kwoty 50 tys. zł, a w stosunku do osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej – 200 tys. zł (zgodnie z art. 121 par. 2 i 3 ustawy o postępowaniu egzekucyjnym w administracji; t.j. Dz.U. z 2014 r. poz. 1619 ze zm.).

W obecnym stanie prawnym, w razie stwierdzenia, że działanie biura rachunkowego ma znamiona przestępstwa, GIODO może zadecy-

dować o przekazaniu sprawy do sądu. Ten może nałożyć kary grzywny, ograniczenia wolności lub pozbawienia wolności do lat 2. Taki katalog kar jest przewidziany przykładowo za przetwarzanie danych mimo zakazu lub przetwarzanie ich przez osobę nieuprawnioną, umyślne ich udostępnianie, brak odpowiednich zabezpieczeń przed zabránieniem bądź udaremnieniem lub utrudnieniem GIODO wykonywania czynności kontrolnej.

Warto zaznaczyć, że unijne rozporządzenie ogólne o ochronie danych osobowych (Dz.Urz. UE z 2016 r. L 119, s. 1), które wejdzie w życie 25 maja 2018 r. i będzie stosowane we wszystkich państwach członkowskich, wyposaży GIODO w uprawnienia do nakładania administracyjnych kar pieniężnych za naruszenie jego przepisów. Kwoty będą mogły sięgnąć nawet 20 mln euro lub, w przypadku przedsiębiorstw, do 4 proc. całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Rozporządzenie zastąpi tym samym ustawę o ochronie danych osobowych.

Podstawa prawna

Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 ze zm.).
Rozporządzenie ministra spraw wewnętrznych i administracji z 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. z 2004 r. poz. 1024).