

Biura rachunkowe w rękach GIODO

Jeżeli generalny inspektor ochrony danych osobowych zakaże przedsiębiorcy prowadzącemu ten rodzaj usług przetwarzania danych osobowych, to tym samym **zakaże mu świadczenia usług**

Agnieszka Pokojka
agnieszka.pokojka@infor.pl

Przedsiębiorcy usługowo prowadzący księgi rachunkowe często nie przestrzegają przepisów ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm.) – twierdzą eksperci i generalny inspektor ochrony danych osobowych. Mimo że nie są prowadzone statystyki dotyczące wyników kontroli GIODO w tych firmach, to można szacować, że problem dotyczy nawet 80 proc. biur rachunkowych.

Brakuje dokumentacji

Według Sławomira Dziudzi-ka, dyrektora Polskiej Izby Biur Rachunkowych, ich właściciele po prostu nie mają świadomości, że ciążą na nich obowiązki dotyczące ochrony danych. Zgodnie z ustawą administrator danych, którym jest klient, może powierzyć ich przetwarzanie innemu podmiotowi, np. biurowi rachunkowemu.

– Musi się to jednak odbyć poprzez podpisanie umowy,

określającej zakres i cel przetwarzania danych – twierdzi dyrektor PIBR. Tymczasem nie wszystkie biura regulują tę kwestię.

Sławomir Dziudzik podkreśla, że fakt, iż odpowiedzialność za zabezpieczenie danych spoczywa na administratorze, nie wyłącza odpowiedzialności podmiotu, któremu je powierzone. Tak więc biuro rachunkowe ma obowiązek zabezpieczenia zbioru danych.

W praktyce większość firm z branży o to nie dba. – Często wchodząc do biura rachunkowego, widzimy półki z dokumentami zawierającymi dane pracowników i kontrahentów klientów biura, brak jest zamykanych szaf – twierdzi Elżbieta Krzyżak, prawnik, audytor wewnętrzny z zakresu bezpieczeństwa, ekspert w dziedzinie ochrony danych osobowych z biura prawnego Agami, Doradztwo i Konsulting.

Ekspert dodaje, że biura rachunkowe często nie wdrożyły podstawowych rozwiązań wynikających z obowiązujących

przepisów, nie mają nawet dokumentacji dotyczącej sposobu przetwarzania danych osobowych. Pracownikom nie wystawiono upoważnień do dostępu do danych. Nikt w firmie nie ma też wiedzy o przetwarzanych zbiorach i o obowiązku zgłaszania ich do rejestru prowadzonego przez GIODO.

Brak zabezpieczeń

Jak wskazuje Elżbieta Krzyżak, problem stanowią też niewieluściwie zabezpieczone systemy komputerowe, brak wdrożenia procesu logowania się do systemu oraz nieprzestrzeganie wymogów co do długości, złożoności i zmiany hasła. Warunki w tym zakresie określa rozporządzenie ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. (Dz.U. nr 100, poz. 1024).

Generalny inspektor ochrony danych osobowych dr Wojciech Rafał Wiewiórowski przyznaje, że zdarzają się przypadki niestosowania odpowiednich zabezpieczeń systemów komputerowych przed atakami z zewnątrz

i dostępem do danych osób nieuprawnionych.

Przepisy wykonawcze do ustawy o ochronie danych osobowych określają trzy poziomy bezpieczeństwa przetwarzania danych w systemach informatycznych. Przykładowo środki bezpieczeństwa na poziomie wysokim stosuje się, gdy co najmniej jedno urządzenie systemu informatycznego wy-

Ważne ▶ Eksperci szacują, że w Polsce działa 30-40 tys. biur rachunkowych. Mogą one obsługiwać nawet ponad 1,5 mln podmiotów gospodarczych

korzystanego do przetwarzania danych osobowych jest podłączone do internetu. – Inny przykład złego zabezpieczenia danych osobowych związany jest z serwisowaniem albo naprawą komputerów. Podczas tych czynności dostęp do danych uzyskują niekiedy osoby do tego nieupoważnione – twierdzi GIODO.

W przypadku np. wadliwie działającego wiatraczka

w komputerze osoba dokonująca naprawy nie powinna mieć dostępu do twardego dysku i zapisanych na nim danych. Wtedy trzeba albo zaszyfrować dane, albo usunąć twardego dysku na czas naprawy sprzętu w serwisie.

Czasem konieczne jest jednak zapewnienie serwisantom dostępu do wszystkich danych zapisanych na dysku, np. gdy zlecona praca ma polegać na naprawie błędów w bazie. – Jeżeli dostęp do danych jest niezbędny do przeprowadzenia naprawy, wówczas z firmą jej dokonującą trzeba zawrzeć umowę powierzenia lub podpowierzenia przetwarzania danych osobowych – wyjaśnia Wojciech Rafał Wiewiórowski.

Zakaz, a nawet sąd

GIODO przyznaje, że nie jest uprawniony do nakładania kar za naruszenie przepisów ustawy o ochronie danych. Jego zadaniem jest dbałość o zgodność z prawem przetwarzanie tych danych. Czyny to m.in. poprzez wydawanie decyzji administracyjnych, w których

– w razie stwierdzenia uchybień – zakazuje przetwarzania danych albo nakazuje wprowadzenie dodatkowych zabezpieczeń czy zmianę sposobu przetwarzania danych.

– Trzeba zdawać sobie sprawę z tego, że jeżeli wydamy decyzję zakazującą biurowi rachunkowemu przetwarzania danych, to tym samym zakażemy mu działalność – podkreśla Wiewiórowski. – Dlatego wówczas, gdy to jest możliwe, wskazujemy błędy i nakazujemy ich usunięcie. Tylko w wyjątkowych sytuacjach zakazujemy przetwarzania danych osobowych, np. do czasu wprowadzenia stosownych zmian.

Informacje o popełnionych przestępstwach GIODO przekazuje do prokuratury. To bowiem do organów ścigania, a następnie do sądów karnych należy decyzja, czy i jakie przepisy prawa zostały naruszone i jaką karę za to nałożyć. Biorąc pod uwagę ustawę o ochronie danych osobowych, może to być grzywna, kara ograniczenia wolności albo pozbawienia wolności do dwóch lat.