

Dane klientów pod ścisłą ochroną

- Małe firmy zbierają dane osobowe konsumentów.
- Wiele z nich nie zabezpiecza tych informacji.
- Za naruszenie obowiązku ochrony grożą surowe sankcje.

EDYTA HOŁDYŃSKA

Przepisy ustawy o ochronie danych osobowych obowiązują wszystkie firmy bez względu na ich wielkość i formę prawną. Zgłoszenie zbioru danych do głównego inspektora ochrony danych osobowych (GIODO) jest – co do zasady – obowiązkiem każdego administratora danych, czyli osoby, która odpowiada za ich gromadzenie i przetwarzanie.

Jedynie w wyjątkowych sytuacjach administratorzy danych są zwolnieni z tego obowiązku. Nie muszą rejestrować w GIODO np. zbiorów danych przetwarzanych w związku z zatrudnieniem (np. zbiorów pracowników), zbiorów danych osobowych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, czy zbiorów danych przetwarzanych w zakresie drobnych bieżących spraw życia codziennego (np. danych kontaktowych do kontrahentów).

Przetwarzanie danych osobowych rozpoczyna się już w momencie ich zbierania. Ale jest ono dopuszczalne tylko w określonych przypadkach. Wolno gromadzić dane, jeśli osoba, której dotyczą, wyrazi na to zgodę lub jeśli jest to koniecz-

ne do realizacji umowy, a także wtedy, kiedy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

W sklepach internetowych tworzona jest np. samoistnie baza klientów i zrealizowanych przez nich transakcji. Zawiera ona dane osobowe i teleadresowe, które należy chronić. Przedsiębiorca jest więc zobowiązany zgłosić zbiór danych do rejestracji GIODO.

Baza podlegająca ochronie powstaje także wtedy, gdy klienci, chcąc otrzymywać gazetki promocyjne czy informacje o wprowadzanych rabatach i wyprzedażach w sklepach, podają swój adres e-mailowy.

Jak przestrzega GIODO, należy zbierać wyłącznie dane ściśle związane z celem prowadzonej działalności gospodarczej. Nie wolno tego robić „na wszelki wypadek”, do przyszłego wykorzystania, ponieważ ich składowanie jest niedozwolone. Zabronione jest także uzależnianie zawarcia umowy od uzyskania zgody na przetwarzanie danych do innych celów, np. marketingowych, osób trzecich.

Nie wolno też wykorzystywać danych osobowych uzyskanych z nieznanego lub niepewnego źródła, niegwarantujących dokładności.



♦ Wolno gromadzić dane, jeśli osoba, której dotyczą, wyrazi na to zgodę lub jeśli jest to konieczne do realizacji umowy

Po osiągnięciu celu przetwarzania (np. po wykonaniu umowy) zebrane dane powinny być usunięte, zanonimizowane lub przekazane podmiotowi upoważnionemu z mocy prawa do ich przejęcia od administratora.

Przepisy ustawy o ochronie danych osobowych i rozporządzenia ministra w sprawie dokumentacji przetwarzania danych osobowych zawierają jedynie ogólne zapisy dotyczące tego, jak należy zabezpieczyć dane osobowe. Przedsiębiorca ma wybór odpowiednich środków gwarantujących im optymalny stopień zabezpieczenia.

– Zastosowane rodzaje zabezpieczeń składają się na tzw. politykę bezpieczeństwa, która powinna zostać opisana przez administratora danych. Natomiast zastosowane zabezpieczenia w systemie informatycznym służącym do przetwarzania danych osobowych administra-

tor danych powinien opisać w specjalnej dokumentacji zwanej instrukcją zarządzania systemem informatycznym – tłumaczy Małgorzata Kałużyńska-Jasak, rzecznik prasowy GIODO.

Ponadto administrator ma obowiązek upoważnić na piśmie każdą osobę przetwarzającą dane osobowe i odnotować ten fakt w prowadzonej ewidencji osób do tego upoważnionych.

Za choćby nieumyślny brak właściwego zabezpieczenia danych przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem grozi grzywna, kara ograniczenia albo pozbawienia wolności do roku. Karze pozbawienia wolności do dwóch lat podlega zaś ten, kto przetwarza w zbiorze dane, choć ich przetwarzanie nie jest dopuszczalne, albo do których przetwarzania nie jest uprawniony. ■