Adam Wojciechowski
Instytut Logistyki i Magazynowania

# Chroń dane osobowe

Logistyka jest dziedziną wiedzy, która wykorzystując nowoczesne metody organizacji i zarządzania, wspomagane systemami informatycznymi, umożliwia kształtowanie optymalnych łańcuchów zaopatrzeniowych od momentu pozyskiwania surowców, poprzez ich przerób, dystrybucję w różnych etapach handlu, aż po nabywcę. Dziedzina ta pozwala na kształtowanie optymalnych łańcuchów dostaw. Panująca na rynku duża konkurencja wymaga wysokiej efektywności działania i profesjonalizmu podczas obsługi klienta, niezależnie od tego, które jest to ogniwo łańcucha. Osiągnięcie wysokiego standardu obsługi klienta nie jest możliwe bez sprawnego funkcjonowania przepływu informacji oraz dokumentów. Aktywne firmy prowadzą działania zorientowane na klienta, które pozwalają na osiągnięcie przewagi konkurencyjnej. Zastosowanie takiego podejścia w interesach nie da się sprawnie i skutecznie realizować bez tworzenia zbiorów danych, niejednokrotnie zawierających dane osobowe potencjalnych klientów, czy też osób wskazanych do kontaktów służbowych w określonych sprawach. Przetwarzanie danych osobowych[1] uregulowane jest w Polsce określonymi uwarunkowaniami prawnymi, do których zalicza się:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133 z 1997, poz. 883, z późniejszymi zmianami),
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,
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Wymagania wynikające z wymienionych aktów prawnych nie są wcale proste do spełnienia dla podmiotów gospodarczych. Zwłaszcza, że odnoszą się one do zbiorów przetwarzanych zarówno

[1] W rozumieniu Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. nr 101 z 2002, poz. 101, z późniejszymi zmianami) danymi osobowymi są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio, a w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

w systemach informatycznych, jak i w kartotekach, skorowidzach, księgach, wykazach itp. zbiorach ewidencyjnych. Interpretacja sformułowań podstawowych wynikających z Ustawy (1) już przysparza wiele wątpliwości i problemów administratorom danych osobowych.

Z Ustawy (1) wynika, jakie zbiory zawierające dane osobowe:
- podlegają obowiązkowi rejestracji u Generalnego Inspektora Ochrony Danych Osobowych (GIODO)
- nie podlegają rejestracji

oraz którzy administratorzy danych[2] są zwolnieni z obowiązku rejestracji przetwarzanych zbiorów danych. Wzór zgłoszenia zbioru danych osobowych do rejestracji GIODO określa Rozporządzenie (3). Jednak poprawna kwalifikacja zbioru danych z całą pewnością także sprawia administratorom danych sporo problemów.

W dobie powszechnej komputeryzacji oraz upowszechnienia komunikacji poprzez Internet administratorzy przetwarzający dane osobowe muszą uporać się z wymaganiami wynikającymi z Rozporządzenia (2), co nie jest takie proste. W myśl tegoż Rozporządzenia administratorzy mają obowiązek posiadania dokumentacji opisującej sposób przetwarzania oraz środków techniczno – organizacyjnych, zapewniających ochronę danych osobowych odpowiednio do zagrożeń i ich kategorii, prowadzonej w formie pisemnej. Dokumentację tę tworzą:
- polityka bezpieczeństwa
- instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Dokument zwany polityką bezpieczeństwa powinien zawierać informacje związane z przetwarzaniem danych:
- wykazujące budynki, pomieszczenia lub ich części stanowiące obszar, gdzie działania te są realizowane
- wykazujące zbiory zawierające dane osobowe i programy wykorzystywane do ich przetwarzania
- opisujące strukturę wskazanych zbiorów, prezentującą zawartość poszczególnych pół informacyjnych i ich powiązań
- określające sposób przepływu danych pomiędzy poszczególnymi systemami
- określające środki organizacyjne i techniczne wymagane w celu zapewnienia przetwarzanym danym odpowiedniej poufności, integralności i rozliczalności.

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, określać powinna:
- procedury związane z:
  – nadawaniem uprawnień osobom przetwarzającym dane osobowe,
  – rejestrowaniem tych uprawnień,
  – odpowiedzialnością osób za te czynności,
- metody i środki stosowane do uwierzytelniania oraz procedury dotyczące ich użytkowana i zarządzana
- tryb postępowania związany z rozpoczynaniem, zawieszaniem i kończeniem prac przy przetwarzaniu danych
- zasady tworzenia kopii zapasowych zbiorów danych, programów i narzędzi wykorzystywanych do ich przetwarzania oraz sposobu, miejsca i okresu ich przechowywania
- formy zabezpieczenia systemu informatycznego przed działaniem oprogramowania umożliwiającego nieuprawniony dostęp do systemu informatycznego
- zasad przeprowadzania przeglądów i konserwacji systemów oraz nośników wykorzystywanych do przetwarzania danych
- sposobu odnotowywania w systemie używanym do przetwarzania danych informacji o odbiorcach w rozumieniu art. 7 pkt. 6 Ustawy (1), którym dane udostępniono, zakresie i dacie danego udostępnienia, za wyjątkiem systemu wykorzystywanego do przetwarzania zbiorów jawnych.

Rozporządzenie (2) określa dla systemów informatycznych trzy poziomy bezpieczeństwa przetwarzania danych osobowych:
- podstawowy dotyczący systemu, w którym nie są przetwarzane dane wskazane w art. 27 Ustawy (1), a urządzenia komputerowe wykorzystywane do przetwarzania danych nie są połączone z siecią publiczną
- podwyższony, dotyczący systemu, w którym przetwarzane są dane wskazane w art. 27 Ustawy (1), a urządzenia komputerowe wykorzystywane do przetwarzania danych nie są połączone z siecią publiczną
- wysoki, dotyczący systemu, w którym chociaż jeden z komputerów wykorzystywanych do przetwarzania danych połączony jest z siecią publiczną, czyli Internetem.

Dla każdego z tych poziomów w Rozporządzeniu (2) określone zostały środki bezpieczeństwa, które powinny zostać spełnione w praktyce. Przy ustalaniu środków bezpieczeństwa przyjęto zasadę, że zasadnicze wymagania sformułowano dla poziomu podstawowego, natomiast na poziomie:
- podwyższonym – administrator zobowiązany jest stosować się do wymagań określonych dla poziomu podstawowego oraz dodatkowo określonych dla podwyższonego
- wysokim – administrator zobowiązany jest stosować się do wymagań określonych dla poziomu podwyższonego oraz dodatkowo określonych dla wysokiego.

Z pełną świadomością można powiedzieć, że aktualnie większość działających na rynku firm powinna dla przetwarzanych danych osobowych zapewnić środki bezpieczeństwa na poziomie wysokim.

Z treści Ustawy (1) dowiemy się, które zbiory zawierające dane osobowe podlegają obowiązkowi rejestracji u GIODO. Wzór zgłoszenia zbioru danych osobowych do rejestracji GIODO określa Rozporządzenie (3). Wskazane jest, aby przed zgłoszeniem zbioru do rejestracji opracowana została wymagana przepisami dokumentacja oraz spełnione zostały warunki techniczne i organizacyjne, wynikające z przytoczonych aktów prawnych. Należy jednak pamiętać, że nawet wtedy, gdy przetwarzamy dane w zbiorach nie podlegających rejestracji, należy spełnić wymagane prawem warunki techniczne i organizacyjne. Oznacza to, że praktycznie każda firma powinna spełniać przedstawione skrótowo warunki prawne i organizacyjne, gdyż jeśli nawet nie gromadziłaby danych osobowych związanych z prowadzonym biznesem, to z całą pewnością posiada zbiory danych osobowych własnych pracowników, które również podlegają Ustawie (1) i Rozporządzeniu (2).

[2] Administrator danych to organ, jednostka organizacyjna, podmiot lub osoba, które decydują o celach i środkach przetwarzania danych osobowych.