

Adam Wojciechowski
Instytut Logistyki i Magazynowania

Dane osobowe podlegają ochronie

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 przeród, dystrybucję w różnych etapach handlu, aż po nabywcę. Mówiąc krócej, jest to dziedzina kształtująca optymalny łańcuch logistyczny. Duża konkurencja na rynku wymaga wysokiej efektywności działania i profesjonalizmu podczas obsługi klienta niezależnie od tego, które jest to ogniwo łańcucha. Osiągnięcie wysokiego poziomu obsługi klienta nie jest możliwe bez sprawnego funkcjonowania przepływu informacji oraz dokumentów. Aktywne, nowoczesne firmy zorientowane są na klienta, który jest dla nich najważniejszy. Na podstawie stosowanych rozwiązań stwierdzono, że bezpośredni kontakt z klientem daje najlepsze efekty w zaspokajaniu jego potrzeb. Przykładem tego jest rosnąca popularność systemów CRM (*Customer Relationship Management*), co w języku polskim oznacza zarządzanie kontaktami z klientem. Podejście ukierunkowane na bezpośredni kontakt sprawia, że wykorzystywane systemy obsługi zawierają zbiory danych o klientach. Wśród tych danych na ogół gromadzone są również dane osobowe, a te podlegają określonym uregulowaniom prawnym.

Podstawowymi dokumentami prawnymi w tym zakresie są:

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133 z 1997, poz. 883, z późniejszymi zmianami) [1]
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 03 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80 z 1998, poz. 521, z późniejszymi zmianami) [2]
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 03

czerwca 1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 80 z 1998, poz. 522) [3].

Spełnienie wymagań wynikających z tych dokumentów nie jest wcale sprawą prostą, gdyż już interpretacja sformułowań podstawowych zawartych w Ustawie [1] przysparza wiele wątpliwości i problemów temu, kto dane osobowe gromadzi.

Już z chwilą zapoznania się z podstawowymi definicjami:

- **dane osobowe** – 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
- **zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie
- **przetwarzanie danych** – jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych
- **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą
- **administrator danych** – organ, instytucja, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 ust. 1 2, decydująca o celach i środkach przetwarzania danych osobowych.
- Każdy z administratorów danych powinien mieć jednak świadomość, że Ustawę [1] stosuje się w odniesieniu do zbiorów

przetwarzanych zarówno w systemach informatycznych, jak i w kartotekach, skorowidzach, księgach, wykazach itp. zbiorach ewidencyjnych.

Poznając dalej treść Ustawy [1] dowiemy się, że zbiory zawierające dane osobowe podlegają obowiązkowi rejestracji u Generalnego Inspektora Ochrony Danych Osobowych (GIODO). Wzór zgłoszenia zbioru danych osobowych do rejestracji GIODO określa Rozporządzenie [3]. Są jednak zbiory danych osobowych, które nie podlegają rejestracji i są administratorzy danych zwolnieni z obowiązku rejestracji przetwarzanych zbiorów danych.

W myśl art. 2 ust 3 Ustawy [1] zbiory danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo podanych anonimizacji, mają zastosowanie jedynie przepisy dotyczące zabezpieczenia, czyli nie podlegają rejestracji.

W art. 43 ust. 1 Ustawy [1] wymieniono dwanaście przypadków zwolnień administratorów danych z obowiązku rejestracji zbioru danych. Spośród tych przypadków, w odniesieniu do przedsiębiorstw obsługujących klienta, wymienić należy zwolnienie zbiorów danych:

- objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa publicznego
- dotyczących osób u nich zatrudnionych, zrzeszonych lub uczących się
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej
- powszechnie dostępnych
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

Prawidłowa kwalifikacja zbioru danych z pewnością sprawi najwięcej kłopotu administratorowi danych.

Po zapoznaniu się z Ustawą [1] wydałoby się, że taki zbiór danych powinien być zarejestrowany u GIODO, gdyż zawiera dane pozwalające zidentyfikować osobę fizyczną, którą jest wspomniany

pracownik. W rzeczywistości, według wykładni prawnej GIODO, dane osób zajmujących kierownicze stanowiska w firmach lub odpowiedzialnych za kontakty służbowe z innymi podmiotami, które są ściśle związane z działalnością zawodową, należy traktować jako dane o charakterze służbowym, do których dostęp osób postronnych jest ułatwiony, czyli są zaliczane do kategorii danych powszechnie dostępnych (art. 43 ust. 1 pkt. 9 Ustawy [1]), nie podlegających rejestracji.

Prawidłowa interpretacja posiadanego zbioru danych osobowych jest bardzo ważna, ponieważ zgodnie z art. 46 Ustawy [1] administrator danych może rozpocząć ich przetwarzanie dopiero po jego zgłoszeniu do GIODO do rejestracji, chyba że jest z tego obowiązku zwolniony. Należy jednak pamiętać o tym, iż zwolnienie zbioru danych osobowych od rejestracji nie zwalnia administratora danych od przestrzegania pozostałych postanowień Ustaw [1].

Stwarza to już kolejny problem do rozwiązania, gdyż obowiązkiem każdego administratora danych jest:

- wydanie upoważnień osobom dopuszczonych do obsługi urządzeń i systemu informatycznego służącego do przetwarzania danych osobowych oraz prowadzenia ewidencji tych osób
- zastosowanie takich środków technicznych i organizacyjnych, które zapewnią ochronę przetwarzanych danych przed dostępem osób nieupoważnionych, za-

braniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem z naruszeniem Ustawy [1].

Dokumentem wykonawczym do Ustawy [1] określającym podstawowe warunki techniczne i organizacyjne jest ww Rozporządzenie [2].

Przed rozpoczęciem przetwarzania administrator danych zobowiązany jest do:

- 1) określenia celu, strategii i polityki zabezpieczenia systemu informatycznego
- 2) identyfikacji oraz analizy zagrożeń i ryzyka, jakie zagraża przetwarzanym danym osobowym
- 3) określenia potrzeb w zakresie zabezpieczenia zbiorów i systemów informatycznych oraz doboru tych zabezpieczeń
- 4) monitorowania funkcjonowania stosowanych zabezpieczeń
- 5) opracowania i wdrożenia programu szkoleń w zakresie zabezpieczeń użytkowanego systemu informatycznego
- 6) przeprowadzania właściwych postępowań w przypadku naruszenia ochrony danych osobowych.

W zakresie należącym do organizacji administrator danych zobowiązany jest do:

- 1) określenia budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe
- 2) opracowania instrukcji określającej sposób zarządzania systemem informatycznym
- 3) określenia zasad tworzenia i postępowania z kopiami awaryjnymi

PRZYKŁAD ZBIORU DANYCH

Przedsiębiorstwo posiada zbiór danych o klientach, który zawiera informacje:

- nazwa przedsiębiorstwa, adres, telefon, fax itp.
- branża, profil produkcji itp.
- imię i nazwisko, stanowisko, telefon i fax pracownika wyznaczonego do kontaktu i uzgodnień w sprawie wykorzystywany jest również do wystawienia faktury oraz przy sporządzaniu sprawozdawczości finansowej.

4) wyposażenia systemu informatycznego w mechanizm uwierzytelniania użytkownika oraz kontroli dostępu do danych.

W zakresie należącym do warunków technicznych administrator danych zobowiązany jest do:

- 1) określenia warunków jakie muszą spełniać budynki lub pomieszczenia, w których przetwarzane są dane
- 2) takiego zagospodarowania i eksploatacji pomieszczeń, aby przetwarzane w nich dane chronione były przed dostępem osób nieupoważnionych
- 3) zapewnienia awaryjnego zasilania energią elektryczną urządzeń i systemu informatycznego, które chroniłoby przed utratą danych
- 4) właściwego postępowania podczas likwidacji i naprawy sprzętu informatycznego, który wykorzystywany był lub jest do przetwarzania danych osobowych.

Zagadnienia dotyczące warunków technicznych i organizacyjnych, jakim

powinny odpowiadać urządzenia oraz systemy informatyczne służące do przetwarzania danych osobowych, przedstawiono skrótowo, ale już na tej podstawie widać złożoność problemu, który należy rozwiązać. Więcej szczegółów w tym zakresie zawiera Rozporządzenie [3]. Każ-

dy administrator danych powinien mieć świadomość, iż tylko dostosowanie się do przepisów wynikających z Ustawy [1] i Rozporządzeń [2] i [3] pozwoli mu uniknąć odpowiedzialności karnej.

Zagadnienia związane z odpowiedzialnością karną za przetwarzanie zbiorów

danych z naruszeniem przepisów precyzuje rozdział 8 Ustawy [1]. Postępowanie niezgodne z przepisami Ustawy [1] jest karalne. Warto wiedzieć, iż w zależności od rodzaju przewinienia może to być grzywna, kara ograniczenia wolności albo pozbawienia wolności nawet do lat 3.