Polityka Bezpieczeństwa

Polityka Bezpieczeństwa Informacji sklepu internetowego Olejowy Raj

Na podstawie przepisów Ustawy z 1 sierpnia 1997 o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych określa się niniejszą Politykę Bezpieczeństwa danych osobowych przetwarzanych w związku z prowadzeniem sklepu internetowego Olejowy Raj

Administrator Bezpieczeństwa Informacji: Kamila Zubrycka kom:534-333-524

Wykaz lokalizacji w których przetwarzane są dane osobowe oraz zastosowane zabezpieczenia

1. Dane osobowe przetwarzane są za pośrednictwem systemu informatycznego w architekturze rozproszonej, przy użyciu serwera znajdującego się w siedzibie firmy Nazwa.pl oraz, na podstawie umowy, serwerów znajdujących się w profesjonalnym centrum przetwarzania danych należącym do Nazwa.pl sp. z o.o. z siedzibą w Krakowie przy ulicy Mieczysława Medweckiego 17.
2. Zastosowano następujące środki ochrony fizycznej danych osobowych:
    a. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
    b. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
    c. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu –
    d. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
    e. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest nadzorowany przez służbę ochrony podczas nieobecności pracowników.
    f. Zastosowano System przeciwpożarowy we wszystkich pomieszczeniach serwerowni.

3. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

    a. Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

b. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
c. Fakt uzyskania dostępu do danych odkładany jest w logach systemowych
d. Zastosowano systemowe środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
e. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
f. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
g. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
h. Użyto system Firewall do ochrony dostępu do sieci komputerowej.

Struktura zbiorów danych osobowych

W ramach systemu informatycznego przetwarzane są dwa zbiory danych osobowych:

1. Zbiór podstawowy sklepu olejowyraj.pl zawierający:
    a. Numer porządkowy
    b. Adres -email
    c. Imię i nazwisko
    d. Adres korespondencyjny
    e. Nr telefonu
    f. Datę rozpoczęcia przetwarzania danych
    g. Flagę wyrażenia zgody na przetwarzanie danych
2. Dane obydwu zbiorów przechowywane są w tabelach bazy danych MySQL, zainstalowanej na zaszyfrowanej partycji serwera wirtualnego. Dostęp do zbioru danych ma wyłącznie administrator danych osobowych oraz osoby przez niego pisemnie upoważnione.
3. Kopia danych osobowych tworzona jest w postaci pliku arkusza kalkulacyjnego Excel (.xls lub .xlsx), a następnie drukowana. Po wydrukowaniu plik zawierający kopię danych osobowych zostaje trwale usunięty z nośnika elektronicznego.

Zadania administratora bezpieczeństwa informacji

Administrator Bezpieczeństwa Informacji:

1. Prowadzi ewidencję osób upoważnionych do dostępu do zbioru danych osobowych
2. Kontroluje prawidłowość przetwarzania danych osobowych
3. Podejmuje odpowiednie działania w przypadku stwierdzenia naruszeń zabezpieczeń

4. Podejmuje odpowiednie kroki w celu zapewnienia ciągłości działania systemów zabezpieczających dane osobowe.

Procedura w przypadku podejrzenia naruszenia zabezpieczeń zbioru danych osobowych

1. Każdy, kto stwierdzi fakt nasuwający podejrzenie wystąpienia możliwości naruszenia bezpieczeństwa informacji zobowiązany jest do niezwłocznego powiadomienia Administratora Bezpieczeństwa Informacji
2. Do czasu przybycia Administratora Bezpieczeństwa Informacji należy:
    a. Niezwłocznie podjąć działanie w celu powstrzymania skutków naruszenia bezpieczeństwa
    b. Ustalić przyczynę naruszenia bezpieczeństwa
    c. Podjąć niezbędne działania w celu udokumentowania przypadku wystąpienia incydentu
    d. Nie opuszczać miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji
3. Administrator Bezpieczeństwa Informacji, po zapoznaniu się z sytuacją podejmuje niezbędne kroki w celu:
    a. Wyjaśnienia incydentu
    b. Ograniczeniu negatywnych skutków incydentu
    c. Zapobieżenia pojawienia się podobnego incydentu w przyszłości
    d. Zgłoszenia wystąpienia incydentu do odpowiednich organów ochrony prawnej, w sytuacji, gdy jest to wymagane dla danego incydentu przez przepisy prawa.