

Ochrona danych osobowych w e-biznesie

Rafał Stępniewski
B2B Consulting Sp. z o.o.



6 sierpień 2013 r.

Definicje

- ∞ Dane osobowe
- ∞ Zbiór danych osobowych (struktura)
- ∞ Przetwarzanie danych osobowych:
 - zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie
- ∞ Czy sprzedając w off-line zbieram dane osobowe?
- ∞ Jakie nowe zbiory danych osobowych dochodzą w e-biznesie?
- ∞ Podstawowe definicje:
 - ADO
 - ABI
 - ASI

Obowiązki

- ☞ Rejestracja zbioru danych osobowych w GODO
- ☞ Polityka Bezpieczeństwa w firmie
 - Instrukcja zarządzania systemem informatycznym
 - Załączniki
 - Oświadczenie
 - Upoważnienie
 - Rejestr osób upoważnionych
 - Raport z naruszenia bezpieczeństwa systemu informatycznego
 - Informacja o zawartości zbioru danych osobowych
- ☞ Wymagania techniczne i organizacyjne
- ☞ Podstawa prawna:
 - Ustawa o ochronie danych osobowych
 - Rozporządzenie MSWiA w sprawie dokumentacji przetwarzania danych osobowych

Wymagania organizacyjne

☞ Administrator danych jest obowiązany

- zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
- powinien zabezpieczyć dane przed
 - ich udostępnieniem osobom nieupoważnionym,
 - zabraniami przez osobę nieuprawnioną,
 - przetwarzaniem z naruszeniem ustawy oraz
 - zmianą, utratą, uszkodzeniem lub zniszczeniem.

☞ Proces i nadawanie uprawnień

- Kontrola dostępu (identyfikatory unikalne + hasło)

Wymagania techniczne

- Wymagania zabezpieczeń – poziom wysoki
 - SSL
 - Hasło (8 znaków min. duże i małe litery + cyfry lub znaki specjalne), zmiana co 30 dni.
 - UPS
 - Zabezpieczenia fizyczne i logiczne
 - Kopie bezpieczeństwa – procedury
 - szyfrowanie dysków (laptop, memory stick)

Co zawiera dokumentacja?

- ⌘ wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- ⌘ wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- ⌘ opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- ⌘ sposób przepływu danych pomiędzy poszczególnymi systemami;
- ⌘ określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Wymagania techniczne

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym

- ∞ daty pierwszego wprowadzenia danych do systemu; (automatycznie)
- ∞ identyfikatora użytkownika wprowadzającego dane osobowe do systemu; (automatycznie)
- ∞ źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
- ∞ informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia; (EOG)

System zapewnia sporządzenie i wydrukowanie raportu zawierającego informacje, o których mowa w ust. 1.

W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

A co z Wordem?

GIODO – rejestracja

- ☞ Wniosek elektroniczny przez stronę WWW
- ☞ Bezpłatny + późniejsze aktualizacje
- ☞ Jakie zbiory muszą rejestrować?
 - Pracownicy
 - Reklamacje
 - Klienci (dwa zbiory)
 - Newsletter
 - CRM

Powierzenie danych

- ✎ Kiedy mamy do czynienia z powierzeniem danych osobowych? (forma pisemna)
- ✎ Komu możemy dane osobowe powierzyć?
- ✎ Czy muszę uzyskać zgodę?
- ✎ Czym się różni powierzenie od przekazania?

Kontrola GIODO

- ✎ Na czym polega?
- ✎ Kiedy się zdarza?
- ✎ Co mi grozi w przypadku nie dopełnienia obowiązków?
 - 200 tys. zł kary,
 - 2 lata pozbawienia wolności
 - 50 tys. zł kary

Co widzi Klient?

Zgody jakie wyraża.

- ✎ Konieczność szyfrowania formularzy (SSL)
- ✎ Polityka prywatności
- ✎ Zgody
 - Jakie i ile zgód na dane osobowe i kiedy?
 - Czy można łączyć zgody?
 - Wszystkie zaznaczone ? (tak jest łatwiej dla Klienta)
- ✎ Oświadczenie woli, nie może być domniemana lub dorozumiana; może być odwołana

Treść zgody powinna zawierać

- ✎ adres siedziby i pełna nazwa, a w przypadku gdy ADO jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- ✎ cel zbierania danych,
- ✎ przewidywanych odbiorców danych,
- ✎ Informację o prawie dostępu do treści danych oraz ich poprawiania,
- ✎ Informację o dobrowolności podania danych

Co w przypadku baz kupionych na rynku?

Inne źródła danych osobowych

Konkursy

- Dane osobowe
- Jakie różnice off-line vs on-line

Programy Lojalnościowe

- Dane osobowe
- Jakie różnice off-line vs on-line

Nowa dyrektywa UE

Zmiany

- ⌘ Dyskusja na temat definicji
- ⌘ Adres IP to też dana osobowa
- ⌘ Bycie zapomnianym w Internecie
- ⌘ Profilowanie – zabronione bez zgody vs praktyka
- ⌘ Większa odpowiedzialność do 1 mln EUR
- ⌘ Ponad 4 tys. poprawek z krajów UE
- ⌘ Uzasadniony interes ADO – pole do nadużyć

B2B Consulting Sp. z o.o.

ul. Ratuszowa 11 lok 628

03-450 Warszawa

Tel. (22) 390 91 05

biuro@rzetelnyregulamin.pl

