



GIODO

Techniczne aspekty zabezpieczenia zbiorów danych osobowych

22 sierpnia 2010

Z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:

Art. 51.

1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Art. 52.

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 53.

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

W 2008r sejm, za rekomendacją rządu, odrzucił projekt nowelizacji ustawy o ochronie danych osobowych. Ów projekt proponował złagodzenie sankcji karnych, poprzez wykreślenie zapisów o pozbawieniu wolności.

Poniższy raport zawiera przegląd kwestii technicznych dotyczących zabezpieczenia zbiorów danych osobowych, w kontekście ich przetwarzania na stronach WWW.

1. Czy adres email jest daną osobową?

Zgodnie z interpretacją GODO sprawa jest jasna: adres email może być uznany za daną osobową, gdy pozwala na zidentyfikowanie osoby fizycznej. Przykładem adresu pozwalającego na identyfikację jest adres w formacie imie.nazwisko@nazwafirm.pl. Internauci cały czas toczą polemikę w tym temacie, jednak stanowisko urzędników jest niezmiennie, a co więcej, logicznie umocowane w ustawie.

2. Czy zbiór adresów email należy zgłaszać jako bazę danych osobowych?

Jak ustaliliśmy, email może być daną osobową. Jeżeli nie jesteśmy w stanie zapewnić, że w tworzonym zbiorze nie pojawi się adres, który spełni taki warunek, to zbiór adresów email powinien być zgłaszany do GODO i podlegać wymaganiom ustawy. Można wyobrazić sobie, automatyczną i ręczną weryfikację adresów, przed ich dodaniem do bazy, jednak niezyciowość takiego rozwiązania jest oczywista.

3. Czy zgoda osoby na przetwarzanie jej danych osobowych jest wymagana?

Jest wymagana (z wyjątkiem opisanym poniżej), chyba że chodzi o usunięcie danych tej osoby ze zbioru. Zgoda nie może domniemana, a więc np. w formularzu na stronie www musi znaleźć się checkbox (lub inny element), którym użytkownik jawnie potwierdza udzielenie zgody. Checkbox nie może być domyślnie zaznaczony. Wspomniany wyjątek, to przypadek, gdy dane są niezbędne do realizacji umowy, np. podczas zakupu w sklepie internetowym, zgoda na przetwarzanie danych nie jest wymagana. Jednak w takim wypadku zakres danych, nie powinien być szerszy niż jest to faktycznie konieczne. W przykładowym sklepie internetowym mogą to być dane niezbędne do wystawienia faktury i wysyłki towaru (imię, nazwisko, adres pocztowy), ale już pytanie użytkownika o płeć czy datę urodzenia, będzie leżało poza zakresem niezbędnych informacji i przetwarzanie tych danych, będzie wymagać zgody.

4. O czym należy poinformować użytkownika, którego dane osobowe będziemy przetwarzali?

Należy poinformować taką osobę o:

- a. adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- b. celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- c. prawie dostępu do treści swoich danych oraz ich poprawiania,
- d. dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

5. **Zabezpieczenie zbioru danych osobowych.**

Minister, w rozporządzeniu o bardzo długiej nazwie (**Dz.U. 2004 nr 100 poz. 1024**) wydzielił trzy poziomy bezpieczeństwa systemów informatycznych, przy czym poziom podstawowy (najniższy) stosuje się tylko w przypadku, gdy w systemie nie są przetwarzane dane osobowe – a więc nie pozostaje on w zakresie naszych rozważań. Interesuje nas natomiast poziom podwyższony i wysoki. Poziom podwyższony powinien być stosowany w przypadku gdy system informatyczny, nie jest połączony z siecią publiczną – co w przypadku aplikacji www jest rzadko spotykane (często nawet sieci firmowe czy inne wewnętrzne, mają punkty styku z siecią publiczną), a poziom wysoki, gdy system jest połączony z siecią publiczną. Jakże wobec tego są te wymagania na poziomie wysokim?

6. **Wymagania techniczne bezpieczeństwa systemu informatycznego na poziomie wysokim.**

- a. Dostęp do danych powinien być kontrolowany – po naszymu, musi być uwierzytelnianie użytkownika.
- b. **Dostęp do danych i wszelkie operacje na nich powinny być logowane:** kto, kiedy, jakie dane dodał, zmienił lub usunął.
- c. Każdy użytkownik mający dostęp do danych powinien posiadać swój własny identyfikator (po naszymu: nazwę użytkownika).
- d. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być ponownie wykorzystany.

- e. Jeżeli uwierzytelniamy użytkowników za pomocą hasła (najczęstszy przypadek) to hasło to powinno mieć minimum 8 znaków, zawierać małe i duże litery oraz cyfry lub znaki specjalne, **a także być zmieniane nie rzadziej niż co 30 dni**. Jak widać system powinien wymuszać zmianę hasła, najpóźniej po 30 dniach od ustawienia poprzedniego.
- f. Dane wykorzystywane do uwierzytelniania, przesyłane przez sieć publiczną, **powinny być szyfrowane** (a więc w przypadku aplikacji webowych pomocne będzie użycie SSLa).
- g. Dane osobowe powinny być zabezpieczone poprzez wykonywanie ich kopii zapasowych. Kopie te powinny być oczywiście przechowywane w sposób uniemożliwiający ich przejęcie, modyfikację, uszkodzenie lub zniszczenie. Powinny być także usunięte niezwłocznie po ustaniu ich użyteczności.

7. Jakie inne dane powinny być przechowywane w zbiorze danych osobowych?

Ze względu na prawa osób, których dane przetwarzamy, powinniśmy dodatkowo przechowywać informacje o:

- a. dacie wprowadzenia danych do zbioru,
- b. sposobu w jaki te dane zebrano.

8. Jakie inne wymagania powinien spełnić system informatyczny?

Oprócz wymagań wymienionych explicite w rozporządzeniu, należy pamiętać, że ustawa nakłada na administratora obowiązek dochowania szczególnej staranności w ochronie powierzonych danych. Dobrą praktyką będzie więc zapewnienie dodatkowych zabezpieczeń, np.:

- a. Szyfrowanie danych osobowych przesyłanych siecią publiczną (a więc szyfrowanie wszelkich formularzy rejestracyjnych, formularzy zmiany danych itp.)
- b. Ograniczenie liczby prób nieudanych logowań do systemu informatycznego
- c. Mechanizmy analizujące i powiadamiające o próbach ataku na system
- d. Ustawienie ograniczonych praw dostępu do plików na serwerze

9. Ochrona danych, a hosting współdzielony

Istnieje powszechna opinia, jakoby w żadnym przypadku nie było możliwości spełnienia wymogów bezpieczeństwa na hostingu współdzielonym – gdzie obok

naszej aplikacji, uruchomionych są dziesiątki innych, a na serwer logują się zupełnie nieznane osoby. Ustawa ani rozporządzenie jednak nie stawiają precyzyjnych wymagań w tej materii, mówią natomiast że rozwiązania z zakresu ochrony danych powinny być dostosowane do zagrożeń oraz kategorii tych danych. W szczególności dane muszą być zabezpieczone przed udostępnianiem, zmianą czy ich utratą. Wydaje się, że poprawnie skonfigurowany serwer obsługujący hosting współdzielony, spełnia te wymagania, co więcej serwery utrzymywane w poważnych centrach danych, którymi operują duże firmy hostingowe, mają szansę być lepiej zabezpieczone niż przypadkowy serwer dedykowany, zarządzany przez niewprawnego administratora. Tak więc zakładam osobiście (nie jest to opinia prawnicza, ale techniczna), że dla wielu typowych rozwiązań (sklepik internetowy, forum itp.) w razie kontroli GIODO można skutecznie obronić się z wykorzystania takiego hostingu. Zadbać należy tylko o wybór sprawdzonego hostingodawcy, z jasną polityką bezpieczeństwa i klarownymi zasadami tworzenia i odzyskiwania kopii zapasowych oraz, opcjonalnie przeprowadzić z zewnątrz test bezpieczeństwa a jego wyniki zachować na wypadek kontroli.

Kontakt

Adam Kubiczek

tel.: +48 602 703 788

email: info@kubiczek.eu

web: www.kubiczek.eu

nip: 634-229-24-57

regon: 278089480

O mnie



Pracę z technologiami internetowymi rozpocząłem w 1998 roku i od tamtego czasu zrealizowałem dziesiątki projektów, zdobywając coraz większe doświadczenie i jednocześnie uświadamiając sobie, że prawdą jest powiedzenie, iż im więcej wiesz, tym więcej nie wiesz. Zdobywanie wiedzy w branży informatycznej wygląda na nieustanną pogoń za króliczkiem, którego nie da się złapać 😊.

Obecnie w zakresie moich zainteresowań leży analiza, rozwijanie i optymalizacja aplikacji internetowych, a także, niejako dla równowagi, programowanie gier we flashu oraz gier i aplikacji dla urządzeń z systemem Android.

Jeżeli chciałbyś zrealizować swój nowy projekt, lub potrzebujesz pomocy przy udoskonaleniu istniejącego produktu - zapraszam do kontaktu.

Serdecznie pozdrawiam

Adam Kubiczek