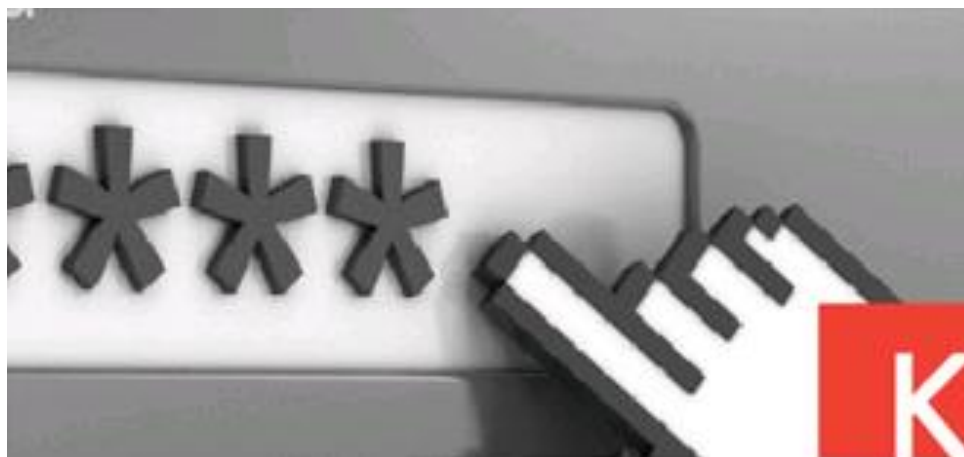


2012

Polityka prywatności

eracity

Celem niniejszego kompendium jest wyjaśnienie, czym jest polityka prywatności i jakie elementy powinna zawierać.



Autor
Fundacja Veracity
2012-06-01



Spis treści

Wprowadzenie	3
Dobre praktyki	3
Odesłania	6



Wprowadzenie

Celem niniejszego poradnika jest wyjaśnienie, czym jest polityka prywatności i jakie elementy powinna zawierać.

Dobre praktyki

Politykę prywatności możemy obecnie znaleźć na każdej szanującej się firmowej stronie, za pomocą, której przetwarzane są informacje dotyczące użytkowników. Warto zaznaczyć, iż jej opisanie i umieszczenie na stronie www jest obowiązkowe tylko w przypadku, gdy za pomocą formularzy umieszczonych na stronie zbierane są dane osobowe. Większość profesjonalnych firm rozszerza jednak zakres polityki prywatności o opis sposobu przetwarzania wszystkich danych pozyskiwanych przez stronę. Z pewnością zwiększa to wiarygodność portalu oraz zaufanie do firmy prowadzącej stronę. Najważniejszym celem polityki prywatności jest zapoznanie klienta z rodzajem danych, jakie będą zbierane oraz celem i sposobem ich przetwarzania. Polityka powinna być umieszczona w takim miejscu, aby użytkownik mógł się z nią zapoznać przed podaniem swoich danych. Zwyczajowo umieszcza się ją na stronie głównej, w stopce lub nagłówku. W żadnych przepisach prawa nie zostało określone, co dokładnie powinna zawierać polityka prywatności. Poniżej przedstawiamy dobre praktyki opracowane na podstawie analizy międzynarodowych wytycznych oraz polityk umieszczonych na stronach wiodących portali przetwarzających dane milionów użytkowników Internetu.

1. Preambuła – zapewniamy klienta o tym, jak ważna jest dla nas ochrona prywatności danych użytkowników.
2. Zakres danych – informujemy użytkowników, jakie dane będziemy zbierali. Warto opisać, jakie dane są dostarczane podczas poszczególnych czynności np.:
 - rejestracja – dane osobowe,
 - zamawianie produktów/usług – dane do faktury,
 - dane zbierane podczas kontaktu telefonicznego, e-maliowego czy też osobistego,
 - dane dotyczące statusu świadczonych za pomocą portalu usług.



Generalna zasada dotyczy zbierania tylko tych danych, które są niezbędne. Im więcej zbieranych danych, tym większe prawdopodobieństwo, iż konieczne będzie spełnienie dodatkowych wymagań narzuconych przez prawo. Użytkownicy powinni zostać powiadomieni zarówno o danych, które sami podają, jak i tych, które są pobierane automatycznie. Jeżeli podanie niektórych danych nie jest obowiązkowe warto to wyraźnie zaznaczyć. W przypadku ewentualnych roszczeń użytkownika będziemy mieli dowód, iż został on poinformowany o tym, że podanie danych było dobrowolne.

3. Cel zbierania danych – informujemy użytkowników, w jakim celu ich dane będą zbierane, np. w celu wysłania zamówienia, wystawienia dokumentów sprzedaży, analizy statystycznej, czy też udostępnienia spersonalizowanych reklam. Jeżeli dane będą udostępniane innym podmiotom (kontrahent, współpracująca firma np. kurier, call center) konieczne trzeba to zaznaczyć w polityce prywatności. Nie ma konieczności podawania nazwy firmy, natomiast należy wskazać grupy, które będą przetwarzały dane osobowe. Informujemy klienta również o możliwości zmiany decyzji w zakresie zgody na przetwarzanie i modyfikacji danych. W przypadku przetwarzania danych osobowych musimy uzyskać od klienta zgodę na ich przekazywanie. Jeśli nie przetwarzamy danych osobowych, wówczas nie mamy obowiązku uzyskania zgody na ich przekazywanie innym podmiotom. W polityce określamy zasady przetwarzania danych klienta. Jeśli klient nie zgadza się na określone zasady, nie powinien korzystać z serwisu. Warto również poinformować, iż w przypadku złamania przez użytkownika prawa lub na wniosek upoważnionych służb, dane będą przekazane uprawnionym organom państwowym.
4. Zmiana danych – dla każdego rodzaju zbieranych danych (patrz pkt. 1) warto opisać sposób ich aktualizacji. Trzeba pamiętać, iż prawnym obowiązkiem jest umożliwienie użytkownikowi wglądu do swoich danych osobowych, aktualizacji, oraz cofnięcia zgody na ich przetwarzanie. W przypadku pozostałych danych jest to dobrą praktyką.
5. Opis stosowanych zabezpieczeń – aby klient czuł, iż jego dane są przetwarzane w bezpieczny sposób, warto go zapewnić o stosowanych zabezpieczeniach. Dotyczy to zarówno etapu transmisji danych między klientem a naszymi serwerami (np. protokół SSL), jak również etapu przetwarzania danych na naszych serwerach. Nie należy szczegółowo opisywać stosowanych zabezpieczeń fizycznych i organizacyjnych. Wystarczy zapewnienie, że dane są zabezpieczone przed nieautoryzowanym



dostępem osób trzecich. Jeśli nasza strona korzysta z rozwiązań w postaci ciasteczek (Cookies) to taką informację, zgodnie z najnowszym prawem telekomunikacyjnym należy umieścić w polityce.

6. Sposób komunikacji z klientem – w polityce prywatności warto wymienić kanały komunikacji wykorzystywane do kontaktu z klientem (e-mail, telefon, korespondencja tradycyjna) oraz określić sposób informowania użytkowników o zmianach dokonanych w polityce prywatności. Dopuszczalne jest umieszczanie informacji dotyczącej zmian w polityce prywatności na stronie, bez indywidualnego informowania użytkowników o dokonanych zmianach. Dobrą praktyką jest pozostawienie archiwalnych wersji polityki, a w przypadku znaczących zmian dodanie krótkiego komentarza, co zostało zmienione i jakie konsekwencje niosą ze sobą wprowadzone zmiany.
7. Nazwa i adres firmy – aby umożliwić kontakt użytkowników z firmą podajemy dane adresowe oraz preferowany sposób kontaktu np.: e-mail, formularz kontaktowy itp.

Jak wcześniej wspomniano, nie ma żadnych wymagań opisujących to, co powinna zawierać polityka prywatności. Każdy zainteresowany powinien dostosować powyższy poradnik do własnych indywidualnych potrzeb. Dobra polityka prywatności powinna być stworzona wspólnie, przez ludzi odpowiedzialnych za aspekty techniczne oraz specjalistów od kontaktu z klientem. Jeśli portal będzie przetwarzał duże ilości danych osobowych warto zasięgnąć również opinii prawników. Trzeba pamiętać, iż polityka prywatności jest tylko dokumentem informacyjnym, a zabezpieczenia techniczne i organizacyjne dla przetwarzania danych osobowych muszą być zgodne z obowiązującym prawem.



Odesłania

1. Rekomendacja R(99) 5 Rady Europy z 23 lutego 1999 r. dotycząca ochrony prywatności w Internecie oraz Aneks do Rekomendacji zawierający wskazówki dotyczące przetwarzania danych osobowych w związku ze zbieraniem i przetwarzaniem danych osobowych w sieciach teleinformatycznych.
2. Dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w Sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej).

