ekonomiawkulturze.pl

Polityka Bezpieczeństwa Danych Osobowych serwisu ekonomiawkulturze.pl przyjęta w dniu 24.10.2012

Wstęp

Opracowanie i wdrożenie Polityki Bezpieczeństwa Danych Osobowych jest jednym z podstawowych warunków legalnego przetwarzania danych osobowych. Obowiązek stworzenia PB określony jest w § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Wolą Operatora Serwisu jest, aby zasady i procedury określone w niniejszym dokumencie były stosowane na wszystkich poziomach przetwarzania danych osobowych, a co się z tym wiąże, miały istotny wpływ na wzrost bezpieczeństwa informacji przetwarzanych przez serwis ekonomiawkulturze.pl.

Cel polityki bezpieczeństwa

Głównym celem jest w szczególności określenie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie ich przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

1. Kryteria bezpieczeństwa

Podstawowymi kryteriami bezpieczeństwa danych osobowych są:

- **integralność** - dane w systemie nie mogą zostać zmienione lub zniszczone przez podmioty nieupoważnione.
- **dostępność** - dane powinny być dostępne i użyteczne (w określonym miejscu, czasie i postaci) dla podmiotów uprawnionych.
- **poufność** - dane nie mogą być udostępniane jakimkolwiek podmiotom nieupoważnionym.

2. Zasady bezpieczeństwa

Zasada rozdziału funkcji i zadań - Funkcje i zadania realizowane w obszarze gromadzenia i przetwarzania danych powinny być oddzielone od funkcji i zadań realizowanych w obszarze bezpieczeństwa informacyjnego.

Zasada wiedzy uzasadnionej - Wszyscy pracownicy posiadają wiedzę o danych zawartych w systemie informatycznym, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych zadań.

Zasada asekuracji zabezpieczeń - Ochrona systemu informatycznego nie powinna być uzależniona wyłącznie od jednego mechanizmu zabezpieczenia, nawet, gdy zastosowana technologia jest uznawana za wysoce zaawansowaną i niezawodną.

Zasada świadomości zbiorowej - Wszyscy użytkownicy systemu informatycznego są świadomi konieczności ochrony wykorzystywanych zasobów.

Zasada indywidualnej odpowiedzialności - za utrzymanie właściwego poziomu bezpieczeństwa poszczególnych elementów systemu informatycznego odpowiadają jego użytkownicy, mający świadomość ponoszonej odpowiedzialności.

3. Podstawy prawne i podstawowe definicje wykorzystywane w Polityce Bezpieczeństwa

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (Dz. U. z 2002, Nr 101, poz. 926 ze zm.),

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),

4. Definicje

Jeżeli w polityce bezpieczeństwa jest mowa o:

- **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych, osobowych takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
- **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ich odtworzenie.
- **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
- **ABI** – rozumie się przez to administratora bezpieczeństwa informacji (art. 36 ust. 3 Ustawy),
- **PB** – rozumie się przez to niniejszy dokument „Polityka Bezpieczeństwa Danych Osobowych portalu ekonomiawkulturze.pl”,
- **Operator Serwisu** – Kamon Consulting – Rafał Kasprzak – przedsiębiorstwo wpisane do ewidencji działalności gospodarczej prowadzonej przez m.st. Warszawę pod numerem 469958, numer NIP 113-176-65-13, numer REGON 141438336, reprezentowane przez Rafała Kasprzaka.
- **Ustawie** – rozumie się przez to Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (Dz. U. z 2002, Nr 101, poz. 926 ze zm.),
- **Rozporządzeniu** – rozumie się przez to Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),

5. Organizacja Bezpieczeństwa Danych osobowych

ABI jest odpowiedzialny za nadzorowanie przestrzegania zasad ochrony danych osobowych. Z zakresu odpowiedzialności ABI wynika, że do jego głównych obowiązków należą:

- aktualizacja dokumentu PB, poprzez jego dostosowywanie do zmieniających się uwarunkowań zewnętrznych, prawnych i technologicznych,
- nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób,
- nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
- nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
- nadzór nad systemem zarządzania hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które powinny być zawarte w instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,

- nadzór czynności związanych ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstotliwości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
- nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
- nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
- nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
- nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowanych przez system informatyczny. W zakresie tego nadzoru, administrator bezpieczeństwa informacji powinien dopilnować, aby osoby zatrudnione przy przetwarzaniu danych osobowych miały dostęp do niszczarki dokumentów w celu niszczenia błędnie utworzonych lub niepotrzebnych już wydruków komputerowych z danymi osobowymi.
- nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych,
- nadzór nad procedurami ustalenia identyfikatorów użytkowników i ich haseł,
- nadzór na procedurami zmiany haseł,
- nadzór nad procedurami dostępu do systemów,
- nadzór na procedurami wyrejestrowania użytkowników z systemu.

Do obowiązków ABI należy również, podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych. Działania, o których mowa wyżej powinny mieć na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie. Do zadań ABI należy także analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie administratorowi danych odpowiednich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

6. Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, został zamieszczony w Załączniku Nr 1 do niniejszego dokumentu.

7. Procedury Bezpiecznej Eksploatacji

Niniejsze procedury zawierają:

A. określenie sposobu przydziału haseł dla użytkowników i sposób ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.
B. określenie sposobu rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.

A. Określenie sposobu przydziału haseł dla użytkowników i sposób ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.

- Prawa dostępu do systemu przydzielane są automatycznie na podstawie login wprowadzonego przez Użytkownika na etapie rejestracji.

- System umożliwia użytkownikowi odzyskanie hasła poprzez kliknięcie na procedurę odzyskiwania hasła.
- W przypadku trudności z realizacją procedury przydziały haseł bądź jego odzyskiwania Użytkownik powinien skontaktować się z Operatorem Serwisu poprzez formularz kontaktowy na stronie http://www.ekonomiawkulturze.pl/home/contact

B. Określenie sposobu rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności,

- Identyfikator wraz z danymi użytkownika podlega rejestracji w systemie informatycznym.
- Dostęp do danych przetwarzanych w systemie informatycznym możliwy jest wyłącznie po podaniu przez użytkownika identyfikatora i właściwego hasła dostępu.
- W przypadku utraty przez użytkownika uprawnień do dostępu do systemu administrator systemu niezwłocznie anuluje uprawnienie dostępu do bazy danych, unieważnia jego hasło oraz podejmuje inne, niezbędne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Nadzór nad realizacją powyższych działań sprawuje ABI.

8. Kopie zapasowe

Kopie bezpieczeństwa są to dane skopiowane na dodatkowe nośniki, pozwalające na odtworzenie w razie awarii tego fragmentu systemu, którego kopie dotyczą. Kopie bezpieczeństwa umieszczane przez przedsiębiorstwo Serveradmin.pl s.c. , które również zajmuje się kopiami bezpieczeństwa i które są one przechowywane w tym samym miejscu co sam serwer.

Załącznik nr 1 do Polityki Bezpieczeństwa Danych Osobowych serwisu ekonomiawkulturze.pl

Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Dane osobowe przetwarzane są w następujących lokalizacjach:

- Siedziba Operatora Serwisu – budynek podlegający całodobowej ochronie oraz monitoringowi. Dane znajdują się w lokalu zabezpieczonym dwoma niezależnymi od siebie certyfikowanymi zamkami.
- Podmiot świadczący usługi hostingowe dla serwisu ekonomiawkulturze.pl – Serveradmin.pl s.c. 35-103 Rzeszów, ul. Staroniowska 73 - budynek podlegający całodobowej ochronie oraz monitoringowi. Dane znajdują się w lokalu zabezpieczonym dwoma niezależnymi od siebie certyfikowanymi zamkami.