INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

obowiązująca u przedsiębiorcy Marcina Chmieleckiego
prowadzącego działalność gospodarczą pod firmą
"CHILI WEB APPLICATIONS" MARCIN CHMIELECKI
z siedzibą w Łodzi przy ul. Traktorowej 126 lok. 104, 91-204 Łódź
NIP: 7261647595, REGON: 472964034

- wersja obowiązująca od dnia 25 maja 2018 roku

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE

1. Niniejszym wprowadza się niniejszą Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych .

2. Jeśli w niniejszej Instrukcję Zarządzania Systemem Informatycznym mowa o:
   a) **Administratorze Danych Osobowych (ADO) –** rozumie się przez to podmiot decydujący o celach i środkach przetwarzania danych osobowych**;**
   b) **Administratorze Systemów Informatycznych (ASI)** – rozumie się przez to osobę fizyczną nadzorującą bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych;
   c) **Haśle** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
   d) **Identyfikatorze użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   e) **Instrukcji** – rozumie się przez niniejszą instrukcję zarządzania systemem informatycznym;
   f) **Odbiorcy danych -** rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów administracji publicznej, które mogą otrzymywać dane osobowe w ramach konkretnego prowadzonego przez nie postępowania;
   g) **Procesorze -** rozumie się przez to Przedsiębiorcę działającego jako podmiot, któremu właściwy ADO powierzył w drodze umowy przetwarzanie danych osobowych**;**
   h) **Przedsiębiorstwie** – rozumie się przez to Marcina Chmieleckiego prowadzącego działalność gospodarczą pod firmą "CHILI WEB APPLICATIONS" MARCIN CHMIELECKI z siedzibą w Łodzi przy ul. Traktorowej 126 lok. 104, 91-204 Łódź, NIP: 7261647595, REGON: 472964034, który pełni rolę Administratora Danych Osobowych lub Procesora lub ;
   i) **Przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   j) **Systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   k) **Usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
   l) **Uwierzytelnianiu** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
   m) **Użytkowniku** – rozumie się przez to osobę, która posiada upoważnienie do przetwarzania danych osobowych i posiada uprawnienia do uwierzytelnionego dostępu do systemu informatycznego;
   n) **Zbiorze danych -** 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.

3. Przedsiębiorca wdraża niniejszą Instrukcję w celu zadośćuczynienia obowiązującym przepisom prawa i zapewnieniu ochrony danych osobowych, które przetwarza jako ADO lub Procesor.

4. Instrukcja odnosi się do danych osobowych przetwarzanych przez Przedsiębiorcę w systemach informatycznych w zakresie jego uprawnień i obowiązków wynikających z łączących go z poszczególnymi ADO umów o powierzenie przetwarzania danych osobowych; część z obowiązków wynikających z powszechnie obowiązujących przepisów może leżeć po stronie tych ADO jako głównych administratorów danych osobowych znajdujących się w danym systemie informatycznym, natomiast Przedsiębiorca jako Procesor wdraża stosowne procedury i zabezpieczenia w odniesieniu do wykonywanego wyłącznie przez niego przetwarzania danych osobowych.

5. Przedsiębiorca zapewnia, że systemy informatyczne zachowują możliwość:
   a) pseudonimizacji i szyfrowania danych osobowych;
   b) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   c) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

6. W toku przetwarzania przez siebie danych osobowych w systemie informatycznym Przedsiębiorca nie stosuje profilowania.

7. Przedsiębiorca zapewnia, że systemy informatyczne są regularne testowane, a skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania mierzona i oceniana.

8. Niezależnie od niniejszej Instrukcji Przedsiębiorca wdrożył Politykę Bezpieczeństwa.

II. PROCEDURY NADAWANIA, MODYFIKOWANIA I USUWANIA UPRAWNIEŃ ORAZ UWIERZYTELNIENIA DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. Przedsiębiorca samodzielnie pełni funkcję ASI.

2. Za nadawanie, modyfikowanie i usuwanie uprawnień Użytkownika do przetwarzania danych osobowych w systemach informatycznych, a także za rejestrowanie takich uprawnień w tymże systemie, odpowiedzialny jest ASI.

3. Uprawnienia dla nowego Użytkownika mogą być nadane wyłącznie osobie upoważnionej do przetwarzana danych osobowych zgodnie z Polityką Bezpieczeństwa.

4. Każdemu Użytkownikowi ASI przyznaje unikalny identyfikator oraz hasło.

5. Identyfikator Użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

6. Użytkownik uwierzytelnia dostęp do systemu informatycznego poprzez wpisanie swojego unikalnego identyfikatora oraz hasła.

7. Zmiana hasła następuje nie rzadziej niż co 30 dni.

8. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

9. Użytkownik ma obowiązek zachować hasło w tajemnicy w czasie jego obowiązywania oraz po ustaniu jego ważności.

10. Użytkownik systemu informatycznego zobowiązany jest niezwłocznie poinformować Przedsiębiorcę i ADO o stwierdzeniu naruszenia zabezpieczeń danych osobowych w systemie informatycznym.

11. ASI może zablokować Użytkownikowi dostęp do systemu informatycznego w każdym czasie, jeśli uzna to za konieczne dla zapewnienia bezpieczeństwa danych osobowych.

12. Po zakończeniu pracy w systemie informatycznym, Użytkownik zobowiązany jest wylogować się z systemu.

13. Identyfikatory i hasła Użytkowników przechowuje się w systemie informatycznym w postaci zaszyfrowanej.

14. Użytkownik, który utracił hasło, zobowiązany jest zgłosić to niezwłocznie ASI, który ustali nowe hasło.

15. Użytkownik zobowiązany jest zapamiętać hasło, o którym mowa wyżej (nie zapisywać go).

III. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. W celu uruchomienia podsystemu informatycznego Użytkownik powinien:
   a) uruchomić komputer;
   b) wybrać odpowiednią opcję umożliwiającą logowanie do systemu;
   c) zalogować się do systemu poprzez wskazanie loginu oraz poufnego i aktualnego hasła.

2. Za każdym razem, kiedy Użytkownik opuszcza stanowisko pracy, zobowiązany jest do wylogowania się z systemu.

3. Użytkownik jest zobowiązany do zapisywania i zamykania wszystkich dokumentów zawierających dane osobowe przed odejściem od komputera.

4. Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj” lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie bez znajomości hasła, dzięki zastosowaniu funkcji wygaszacza ekranu.

IV. PROCEDURY TWORZENIA KOPII ZAPASOWYCH

1. Kopie zapasowe zbiorów danych osobowych tworzone są codziennie po zakończonym dniu pracy ze zbiorem, chyba że danego dnia nie dokonano żadnych zmian w zbiorze.

2. Kopie zapasowe są wykonywane za pomocą oprogramowania Przedsiębiorcy.

3. Za tworzenie kopii zapasowych odpowiedzialny jest ASI lub wyznaczona przez niego osoba posiadająca upoważnienie do przetwarzania danych osobowych.

V. PROCEDURY PRZECHOWYWANIA NOŚNIKÓW DANYCH ORAZ KOPII ZAPASOWYCH

1. Kopie zapasowe systemów informatycznych nie mogą być zbywane ani przekazywane podmiotom nieuprawnionym.

2. Kopie zapasowe systemów informatycznych zawierające dane osobowe przechowywane są na własnym serwerze Przedsiębiorcy.

3. Kopie zapasowe systemów informatycznych, po ustaniu ich przydatności, są usuwane w sposób wykluczający ich odtworzenie.

VI. ZABEZPIECZENIE SYSTEMÓW INFORMATYCZNYCH

1. Przedsiębiorca stosuje w systemie informatycznym jak najbezpieczniejsze dostępne systemy operacyjne.

2. Systemy informatyczne są zabezpieczone przed atakami z zewnątrz za pomocą oprogramowania typu firewall.

3. Systemy informatyczne są zabezpieczone przed szkodliwym oprogramowaniem za pomocą aktualnego oprogramowania antywirusowego.

4. Użytkownicy nie mogą używać prywatnego sprzętu przenośnego, takiego jak płyt CD i DVD, pamięci masowych USB na komputerach, przy użyciu których, przetwarza się dane osobowe. Dotyczy to również podłączania do komputera telefonów komórkowych.

5. Użytkownicy, w przypadku korzystania przy przetwarzaniu danych osobowych z komputerów przenośnych, mają obowiązek zapewnić przechowywać i użytkować komputer przenośny w sposób wykluczający jego uszkodzenie skutkujące usunięciem lub uszkodzeniem danych osobowych oraz przed dostępem osób trzecich.

6. W celu przeciwdziałania atakom zainfekowanych plików, system musi być skanowany przynajmniej raz dziennie pod kątem obecności w systemie wirusów i innych zagrożeń.

7. W przypadku wykrycia jakiegokolwiek zagrożenia Użytkownik niezwłocznie zawiadamia ASI.

8. W przypadku stwierdzenia braku zasilania należy zapisać dane osobowe oraz wylogować się.

9. Ekrany komputerów, na których przetwarzane są dane osobowe, należy chronić wygaszaczami zabezpieczonymi hasłem.

10. Monitory komputerów należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych, w szczególności nie mogą one być zwrócone w stronę okien i drzwi.

11. Użytkownik systemu zobowiązany jest do prawidłowej eksploatacji powierzonego sprzętu i oprogramowania oraz ochrony zasobów informatycznych przed dostępem osób nieupoważnionych, w tym zabezpieczenia komputerowych stanowisk dostępu do danych osobowych przed wglądem osób nieupoważnionych, zabezpieczenia danych przed ich zmianą.

VII. INFORMACJE ODNOTOWYWANE PRZEZ SYSTEM INFORMATYCZNY

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – System informatyczny zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu;
   b) identyfikatora Użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   d) informacji o odbiorcach danych, którym dane osobowe zostały udostępnione, oraz dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
   e) wniesienia przez osobę, której dane są przetwarzane, sprzeciwu w przypadkach przewidzianych w stosownych przepisach.

2. Odnotowanie informacji, o których mowa w rozdziale VII ust. 1 pkt 1 i 2 niniejszej Instrukcji, następuje automatycznie po zatwierdzeniu przez Użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu

zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w rozdziale VII ust. 1 niniejszej Instrukcji.

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

VIII. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW INFORMATYCZNYCH

1. Przynajmniej raz w roku wykonuje się przegląd Systemu informatycznego.

2. Konserwacji poszczególnych elementów Systemu informatycznego dokonuje się tak często, jak to wynika z ich specyfiki – nie rzadziej niż raz w roku.

3. Przeglądy i konserwacje ewidencjonuje się w Załączniku nr 2 do niniejszej Instrukcji.

4. W przypadku awarii systemu informatycznego lub nośników informacji naprawia się je lub odzyskuje dane z zachowaniem tajemnicy danych osobowych zgodnie z Polityką Bezpieczeństwa.

5. Gdy niemożliwa jest naprawa Systemu informatycznego, jego elementu lub nośnika danych, w celu przywrócenia sprawności działania systemu należy zastąpić go nowym oraz posłużyć się kopią zapasową.

6. W przypadku przekazania innym podmiotom elementów Systemu informatycznego lub nośnika danych w celu naprawy, wszelkie dane osobowe muszą zostać z nich usunięte albo należy zabezpieczyć umieszczone na nim dane osobowe przed dostępem podmiotów trzecich.

IX. POSTANOWIENIA KOŃCOWE

1. Przypadki nieuzasadnionego zaniechania obowiązków lub naruszenia innych zasad wynikających z niniejszej Instrukcji mogą stanowić podstawę do pociągnięcia danej osoby do odpowiedzialności, adekwatnie do łączącego ją z Przedsiębiorcą stosunku prawnego.

2. W sprawach nieuregulowanych niniejszą Instrukcję oraz Polityką Bezpieczeństwa mają zastosowanie stosowne przepisy.

XII. WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1 Ewidencja przeglądów i konserwacji