

POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH
OSOBOWYCH

gromadzonych przez CodeRex Adrian Kwiatkowski

REGON: 364861384, NIP: 5361885525

Adres siedziby: ul. Leśna 6 m 35, 05-120 Legionowo

Spis treści

1.Cel polityki.....	2
2.Podstawa prawna.....	3
3.Definicje.....	4
4.Podmioty odpowiedzialne za realizację Polityki Bezpieczeństwa.....	6
5.Administracja i organizacja bezpieczeństwa.	7
6.Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.....	8
7. Wykaz zbiorów danych osobowych oraz sposobu ich gromadzenia.....	9
8.Dane osobowe gromadzone w formie papierowej	10
9.Dane osobowe gromadzone w formie elektronicznej.....	11
10. Bezpieczeństwo fizyczne, sprzętu i oprogramowania.	13
12. Postanowienia końcowe.....	13
13. Wykaz załączników.....	14

Cel polityki.

Celem niniejszego dokumentu jest określenie zasad bezpieczeństwa przetwarzania danych osobowych oraz przedstawienie informacji z zakresu ich ochrony, wobec ich gromadzenia przez CodereX Adrian Kwiatkowski.

Poprzez ochronę danych osobowych rozumie się:

- a) ochronę przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabránieniem przez osobę nieuprawnioną;
- b) przetwarzaniem ich z naruszeniem prawa;
- c) ochrona przed ich utratą, uszkodzeniem lub zniszczeniem;

W dokumencie przedstawiono podstawy prawne dotyczące przetwarzania danych osobowych oraz przedstawiono zasady postępowania na wypadek wystąpienia naruszenia bezpieczeństwa.

Dokument opracowano w celu zwiększenia świadomości obowiązków i odpowiedzialności przedsiębiorcy, a tym samym skuteczności ochrony przetwarzanych zasobów. Poniżej zostały przedstawione zasady organizacji pracy przy zbiorach osobowych przetwarzanych w systemie informatycznym wyrażone w Polityce bezpieczeństwa oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Wszystkie dokumenty uzupełniające treść niniejszej Polityki Bezpieczeństwa zebrano w postaci załączników, które stanowią jej integralną część.

Podstawa prawna.

Niniejszą Politykę Bezpieczeństwa przetwarzania danych osobowych gromadzonych przez CodereX Adrian Kwiatkowski opracowano w związku z:

- Rozporządzeniem 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),
- Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) – art. 46a ustawy,

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
- Wytycznymi w zakresie opracowania i wdrożenia polityki bezpieczeństwa opracowanymi przez Generalnego Inspektora Ochrony Danych Osobowych.

Niniejszy dokument powstał w oparciu o art. 36 ust. 2 oraz art. 39a Ustawy o Ochronie Danych Osobowych, które zobowiązują Administratora danych do wykonania dokumentacji opisującej środki organizacyjne i techniczne służące ochronie przetwarzanych danych osobowych. Szczegółowy zakres dokumentu określa 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 wydane do art. 39a ustawy.

Definicje.

- 1) **Polityka bezpieczeństwa** - zbiór spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których przedsiębiorca Adrian Kwiatkowski buduje, zarządza oraz udostępnia zasoby, systemy informacyjne, informatyczne i dokumentację gromadzoną w związku z funkcjonowaniem swojego przedsiębiorstwa. Określa ona, które zasoby i w jaki sposób mają być chronione.
- 2) **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej 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.
- 3) **Dane wrażliwe** – grupa szczególnie chronionych danych osobowych, do których zalicza się: dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
- 4) **Dane osobowe powierzone do przetwarzania** – dane osobowe o których w pkt. 3.2. które zostały powierzone do przetwarzania Administratorowi Danych Osobowych przez podmiot

trzeci. Do powierzenia przetwarzania danych osobowych dochodzi w drodze zawartej umowy w formie pisemnej.

- 5) **Administrator Danych Osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. W rozumieniu niniejszego dokumentu Administratorem Danych Osobowych jest Adrian Kwiatkowski prowadzący działalność gospodarczą pod firmą CodereX Adrian Kwiatkowski, NIP: 5361885525, REGON 364861384, adres siedziby: ul Leśna 6 m 35, 05-120 Legionowo, tel. 510914326, adrian@codereX.pl;
- 6) **Administrator Bezpieczeństwa Informacji (ABI)** - osoba nadzorująca z upoważnienia Administratora Danych Osobowych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną. Administrator Bezpieczeństwa Informacji w przedsiębiorstwie ADO nie będzie powoływany.
- 7) **Administrator Systemu Informatycznego (ASI)** – osoba albo podmiot odpowiedzialne za działanie oraz zabezpieczenie systemu informatycznego odpowiedzialną za bezpieczeństwo danych osobowych. Administrator Systemu Informatycznego w przedsiębiorstwie ADO nie będzie powoływany.
- 8) **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- 9) **Przetwarzanie danych** - jakiegokolwiek operacje wykonywane na danych osobowych gromadzonych przez ADO bądź przekazanych ADO do przetwarzania na podstawie odrębnej umowy. Przykładowe operacje wykonywane na danych osobowych to pobieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a także te, które wykonuje się w systemach informatycznych.
- 10) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- 11) **Użytkownik** – rozumie się przez to osobę uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz kartotekach, posiadającą ustalony identyfikator i hasło.

- 12) **Pomieszczenia** - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.
- 13) **Zabezpieczanie danych w systemie informatycznym** – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- 14) **Usuwanie danych** – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
- 15) **Zgoda osoby, której dane dotyczą** – należy przez to rozumieć oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli innej treści.
- 16) **Odbiorcy danych** – należy przez to rozumieć każdego, komu udostępnia się dane osobowe, z wyłączeniem:
- osoby, której dane dotyczą,
 - osoby upoważnionej do przetwarzania danych,
 - przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz. U. z 1997 r. Nr 133, poz. 883; tekst jednolity: Dz. U. z 2002 r., Nr 101, poz. 926),
 - podmiotu, o którym mowa w art. 31 ww. Ustawy,
 - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Podmioty odpowiedzialne za realizację Polityki Bezpieczeństwa.

- 1) Podmiotem odpowiedzialnym za realizację Polityki Bezpieczeństwa jest Administrator Danych Osobowych.
- 2) Do obowiązków Administratora Danych Osobowych należy:
 - a. wdrażanie postanowień Polityki Bezpieczeństwa,
 - b. nadzorowanie innych osób przetwarzających dane w zakresie realizacji Polityki Bezpieczeństwa,

- c. nadzorowanie zabezpieczeń Danych Osobowych,
- d. czuwanie nad prawidłowością przetwarzania Danych Osobowych,
- e. wydawanie upoważnień pracownikom do przetwarzania Danych Osobowych,
- f. prowadzenie ewidencji pomieszczeń służących do przetwarzania Danych Osobowych,
- g. aktualizacja Polityki Bezpieczeństwa,
- h. dokonywanie zgłoszeń rejestracyjnych oraz aktualizacyjnych Danych Osobowych,
- i. podejmowanie interwencji w przypadku stwierdzenia naruszenia Polityki Bezpieczeństwa lub zagrożenia dla przetwarzanych Danych Osobowych.
- j. zarządzanie Systemem Informatycznym,
- k. wdrażanie rozwiązań technicznych w Systemie Informatycznym służących ochronie Danych Osobowych,
- l. bieżąca konserwacja i nadzór nad prawidłowym działaniem Systemu Informatycznego,
- m. przydzielanie uprawnień do przetwarzania danych w Systemie Informatycznym,
- n. odbieranie uprawnień do przetwarzania danych w Systemie Informatycznym,
- o. rejestrowanie naruszenia przepisów prawa lub Polityki Bezpieczeństwa w Systemie Informatycznym;
- p. przygotowanie kopii danych osobowych oraz ich zabezpieczenie,
- q. zabezpieczenie nośników z danymi osobowymi,
- r. nadzorowanie likwidacji nośników danych osobowych,
- s. prowadzenie ewidencji upoważnionych pracowników,

Administracja i organizacja bezpieczeństwa.

Za bezpieczeństwo i ochronę danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych i podmiot, któremu na mocy załączonej umowy na powierzenie przetwarzania danych osobowych zostało powierzone część obowiązków (Załącznik nr 11). Administrator Danych Osobowych zobowiązany jest we własnym

Dokument przeznaczony do użytku wewnętrznego przedsiębiorstwa CodereX Adrian Kwiatkowski, REGON: 364861384. Wszelkie kopiowanie oraz rozpowszechnianie bez zgody LS Polska Przemysł Puzdrowski jest zakazane

zakresie stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych wykorzystywanych do działań związanych z działalnością przedsiębiorstwa. W szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Administrator Danych Osobowych oraz jego pracownicy zapoznali się z regulacjami dotyczącymi ochrony danych osobowych stosowanych w przedsiębiorstwie ADO, w szczególności poprzez zapoznanie się z Polityką bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach działalności przedsiębiorstwa ADO które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

- 1) W zakresie wskazanym w umowie na powierzenie przetwarzania danych osobowych, dane osobowe będą gromadzone i przetwarzane przez Fakturownia sp. z o.o. z siedzibą w Warszawie. W pozostałym zakresie dane osobowe przetwarzane będą w siedzibie głównej przedsiębiorstwa ADO mieszczącej się w Legionowie przy ul. Leśnej 6 m 35.
- 2) W siedzibie głównej przedsiębiorstwa znajduje się tylko jedno pomieszczenie i jest nim biuro.
- 3) Siedziba główna przedsiębiorstwa ADO jest zabezpieczona przed dostępem osób trzecich przez drzwi zamykane na klucz.
- 4) Pomieszczenia, w których przetwarzane są dane osobowe są zamykane na klucz podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do niego osobom nieupoważnionym;
- 5) Osoba upoważniona zobowiązana jest do zamykania na klucz pomieszczeń, w których przetwarzane są dane osobowe w czasie jej chwilowej nieobecności w miejscu pracy. Klucze nie mogą być pozostawione w zamku drzwi. Nie można wynosić ww. kluczy po zakończeniu pracy poza miejsca przeznaczone do ich przechowywania.

Wykaz zbiorów danych osobowych oraz sposobu ich gromadzenia.

- 1) ADO przetwarza dane osobowe: swoich kontrahentów (klientów oraz dostawców), pracowników oraz osób których dane osobowe zostały mu przekazane do przetwarzania w drodze zawartych umów na powierzenie przetwarzania danych osobowych.
- 2) Dane osobowe gromadzone są wyłącznie w postaci elektronicznej;
- 3) Dane w wersji elektronicznej są przetwarzane i przechowywane w zależności od ich charakteru:
 - Dane osobowe klientów w wersji elektronicznej gromadzone za pośrednictwem strony internetowej działającej pod adresem www.cinkchat.pl są przetwarzane i przechowywane przez ADO na serwerach dzierżawionych od ObjectLabs Corporation. Wykaz zabezpieczeń stosowanych przez ObjectLabs Corporation jest wskazany pod adresem <http://docs.mlab.com/security>;
 - Dane osobowe klientów w wersji elektronicznej gromadzone w celu sprawozdawczości finansowej są przetwarzane i przechowywane przez Fakturowania sp. z o.o. z siedzibą w Warszawie zgodnie z umową na powierzenie przetwarzania danych osobowych stanowiącej załącznik nr 10.
 - Dane osobowe klientów w wersji elektronicznej gromadzone w sposób inny niż wskazany powyżej (dane elektroniczne przetwarzane na dyskach twardej komputery ADO) przechowywane są według zasad wskazanych w niniejszej polityce bezpieczeństwa.

Dane Osobowe gromadzone w formie elektronicznej

- 1) Administrator Danych Osobowych zbiera dane osobowe w formie elektronicznej w następujących zbiorach (wraz z wskazaniem podziału na grupy wg. których dane osobowe są dzielone)
 - Klienci (grupy: Klienci);
 - Zainteresowani (Grupy: Użytkownicy, Newsletter);
 - Pracownicy (Grupy: Pracownicy);
 - Dane powierzone do przetwarzania (Grupy: Historia rozmów w aplikacji Cink)
- 2) Dane osobowe klientów w wersji elektronicznej są gromadzone w następujący sposób:

- Klienci (Powierzone*, Komputer ADO 1**, serwer zewnętrzny***);
- Zainteresowani (Komputer ADO 1**, serwer zewnętrzny***);
- Pracownicy (Komputer ADO 1**, serwer zewnętrzny***);
- Dane powierzone do przetwarzania (Komputer ADO 1, serwer zewnętrzny***)

*- Powierzone – dane są gromadzone przez podmiot, któremu ADO powierzył przetwarzanie części danych w drodze umowy na powierzenie przetwarzania danych osobowych stanowiącej załącznik nr 11

** Komputer ADO 1 – komputer znajdujący się w siedzibie ADO;

*** serwer zewnętrzny – serwer dzierżawiony przez ADO od ObjectLabs Corporation;

3) Wykaz programów komputerowych służących do przetwarzania i gromadzenia danych osobowych w formie elektronicznej (wraz z wskazaniem zbiorów danych, które są przetwarzane przez te programy);

- Linux (zbiory danych: Klienci, Zainteresowani, Pracownicy, Dane powierzone do przetwarzania);
- MongoDB Compass (zbiory danych: Dane powierzone do przetwarzania)
- RoboMongo (zbiory danych: Dane powierzone do przetwarzania)

4) Zakres danych osobowych gromadzonych w każdym zbiorze:

- Klienci (Imię i Nazwisko, Adres, Adres dla doręczeń, Numer telefonu, Adres E-mail, Adres IP, NIP, REGON, Nazwa Przedsiębiorstwa)
- Zainteresowani (Adres E-mail, Adres IP,)
- Pracownicy (Imię i nazwisko, PESEL, Adres, Adres E-mail, Karta Pracy)
- Dane powierzone do przetwarzania (Adres e-mail, Adres IP, Imię i Nazwisko)

5) Systemy Informatyczne stosowane przez Administratora Danych Osobowych:

- System Informatyczny strony internetowej działającej pod adresem www.cinkchat.com;
- System informatyczny wykorzystywany przez ObjectLabs Corporation w zakresie w jakim jest to niezbędne do udostępniania i funkcjonowania serwera udostępnianego na rzecz ADO;
- System informatyczny wykorzystywany w komputerze ADO;

6) Sposób przepływu danych pomiędzy poszczególnymi systemami

- Dostęp do danych internetowych gromadzonych przez stronę internetową działającą pod adresem www.cinkchat.com ma każdy kto posiada login oraz hasło umożliwiające zalogowanie się do panelu zarządzającego. Dane osobowe gromadzone za pośrednictwem strony internetowej www.cinkchat.com nie są przesyłane do programów wykorzystywanych przez ADO. Dane osobowe z programów wykorzystywanych przez ADO nie są przesyłane do systemu informatycznego udostępnianego za pomocą panelu administracyjnego strony internetowej.
- W sieci lokalnej nie są udostępniane dane z poszczególnych zbiorów. Dane te nie są udostępniane pozostałym systemom informatycznym.
- Serwer dzierżawiony przez ADO od ObjectLabs Corporation jest udostępniany na rzecz wszystkich komputerów ADO, a dostęp do niego mają osoby upoważnione – posiadające login i hasło. Serwer ADO nie udostępnia danych osobowych pozostałym systemom informatycznym. W serwerze dzierżawionym przez ADO są przetwarzane następujące zbiory danych osobowych: Klienci, Zainteresowani, Pracownicy, Dane powierzone do przetwarzania

7) Systemy informatyczne zapewniają wysoki poziom bezpieczeństwa przetwarzania danych osobowych, w rozumieniu Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

8) Przekazanie danych osobowych poza siedzibę firmy odbywa się w sposób zapewniający ich ochronę.

9) Zakres przesyłanych danych osobowych i sposób ich przesyłania u ADO szczegółowo określa Instrukcja Zarządzania Systemem Informatycznym.

Bezpieczeństwo fizyczne, sprzętu i oprogramowania.

- 1) Pomieszczenie, w którym znajduje się komputer jest zamknięte, jeśli nikt w nim nie przebywa.
- 2) Sprzęt i oprogramowanie posiadają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej, w związku z tym powinny być przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.
- 3) Nie dozwolonym jest korzystanie z jakiegokolwiek oprogramowania bez zgody Administratora Danych Osobowych. Dodatkowe oprogramowanie może być instalowane wyłącznie po uzyskaniu pozwolenia.
- 4) Poszczególne stacje robocze powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (bateria od laptopa/zasilacz UPS) co umożliwia funkcjonowanie systemu w przypadku awarii zasilania.
- 5) W celu zabezpieczenia ciągłości pracy, ADO wykonuje okresowo kopię danych osobowych.
- 6) Ochronę przed wirusami stanowi oprogramowanie antywirusowe – AVG Free Edition for Linux.

Postanowienia końcowe.

- 1) Niniejsza Polityka powinna być weryfikowana przynajmniej raz do roku przez Administratora Danych.
- 2) Treść Polityki jest aktualizowana w przypadku wprowadzenia lub zmiany środków technicznych lub organizacyjnych służących ochronie danych osobowych.
- 3) Po dokonaniu aktualizacji tworzy się nową wersję Polityki nadając jej kolejny numer.
- 4) Zasady polityki bezpieczeństwa danych osobowych jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
- 5) Użytkownik zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
- 6) Polityka wchodzi w życie z dniem jej podpisania.

Wykaz załączników.

- 1) Załącznik nr 1. Wykaz przetwarzanych zbiorów osobowych.
- 2) Załącznik nr 2. Wykaz miejsc przetwarzania zbiorów osobowych.
- 3) Załącznik nr 3. Wykaz osób upoważnionych do przetwarzania danych osobowych.
- 4) Załącznik nr 4. Wzór upoważnienia do przetwarzania danych osobowych.
- 5) Załącznik nr 5. Wzór unieważnienia upoważnienia do przetwarzania danych osobowych.
- 6) Załącznik nr 6. Wzór potwierdzenia znajomości zasad bezpieczeństwa.
- 7) Załącznik nr 7. Wzór zgody na przebywanie w obszarze przetwarzania danych osobowych.
- 8) Załącznik nr 8. Wzór odwołania zgody na przebywanie w obszarze przetwarzania danych osobowych.
- 9) Załącznik nr 9. Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych.
- 10) Załącznik nr 10. Wzór zgody na przetwarzanie danych.
- 11) Załącznik nr 11. Umowa na powierzenie przetwarzania danych osobowych.