POLITYKA BEZPIECZEŃSTWA

W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W SKW Spółka z ograniczoną odpowiedzialnością

Spis treści

1. PODSTAWA PRAWNA

Niniejsza „Polityka bezpieczeństwa” stanowi wykonanie obowiązku, o którym mowa w § 4 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. z 2004 r. Nr 100, poz. 1024).

2. CEL OPRACOWANIA DOKUMENTU

1. Celem opracowania niniejszego dokumentu jest wytyczenie zasad i wymagań w zakresie ochrony danych osobowych gromadzonych i przetwarzanych SKW Spółka z ograniczoną odpowiedzialnością w Gdynia (dalej „SKW”), biorąc pod uwagę, że w jednostce organizacyjnej nie został powołany Inspektor Ochrony Danych. Ponadto, celem niniejszej Polityki Bezpieczeństwa jest ochrona danych osobowych, przetwarzanych przez SKW w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem. Wypracowane zasady i wymagania mają ukierunkować działania zmierzające do budowy systemu bezpieczeństwa, a potem jego utrzymywania podczas eksploatacji, na poziomie odpowiadającym potrzebom organizacji.

2. Dokument ten jest również wyrazem świadomości SKW wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających swoje dane osobowe. Mając to na uwadze SKW deklaruje:
   1) zamiar podejmowania wszelkich działań niezbędnych do ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,
   2) zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w firmie w zakresie problematyki bezpieczeństwa danych,
   3) zamiar traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonywania przez zatrudnione osoby,
   4) zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych

3. Polityka Bezpieczeństwa Informacji będzie weryfikowana i dostosowywana w celu zapewnienia odpowiedniego poziomu bezpieczeństwa.

4. Przeglądy dokumentacji Polityki Bezpieczeństwa odbywają się nie rzadziej niż raz w roku.

3. PODSTAWOWE DEFINICJE

1) **Administrator danych** – SKW Spółka z ograniczoną odpowiedzialnością z siedzibą w Gdyni (dalej jako: „SKW”),
2) **dane osobowe** – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej , możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
3) **dostępność danych** – właściwość gwarantująca, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie
4) **informatyczne nośniki danych** – materiały lub urządzenia służące do zapisywania, przechowywania i odczytywania danych osobowych w postaci cyfrowej lub analogowej,
5) **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
6) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
7) **przetwarzanie danych osobowych** – jakiekolwiek operacje lub zestaw operacji wykonywane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, porządkowanie, przeglądanie, pobieranie, udostępnianie, rozpowszechnianie, dopasowywanie lub łącznie, ograniczanie, usuwanie i niszczenie,
8) **rozliczalność danych** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
9) **rozporządzenie** – 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. z 2004 r. Nr 100, poz. 1024),
10) **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922) oraz ustawa z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000) w części w jakiej uchyliła przepisy pierwszej ustawy,
11) **RODO -** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
12) **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą (”anonimizacja”),
13) **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
14) **zarządzanie ryzykiem** – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy za-chowaniu akceptowalnego poziomu kosztów.

4. CELE I STRATEGIE POLITYKI BEZPIECZEŃSTWA

1. Głównym celem Polityki bezpieczeństwa jest ochrona danych osobowych, przetwarzanych przez SKW, w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

2. Ponadto w dziedzinie bezpieczeństwa informacji SKW zamierza realizować następujące **cele**:
   1) zgodność z prawem,
   2) ochrona zasobów informacyjnych,
   3) ochrona wizerunku SKW,
   4) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów, rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,
   5) zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty bezpieczeństwa,
   6) zapewnienie odpowiedniego poziomu wiedzy dotyczącej bezpieczeństwa informacji wśród pracowników i współpracowników SKW,

3. Powyższe cele osiągane są m.in. przez realizowane **strategie**:
   1) właściwą organizację systemu ochrony danych w SKW,
   2) zarządzanie ryzykiem w celu ograniczania go do akceptowanego poziomu bezpieczeństwa,
   3) właściwą ochrona informacji, a w szczególności informacji prawnie chronionych,
   4) zapewnienie odpowiedniego poziomu dostępności informacji i niezawodności systemów informatycznych,
   5) właściwą ochronę informacji związanych z zawartymi umowami,
   6) wdrażanie, eksploatacja i rozwój systemów informacyjnych z zachowaniem zasad bezpieczeństwa,
   7) stała edukacja użytkowników systemu informacyjnego,
   8) okresowe przeglądy (audyty) w zakresie ochrony danych osobowych.

5. ZAKRES STOSOWANIA POLITYKI BEZPIECZEŃSTWA

1. W ramach zabezpieczenia danych osobowych ochronie podlegają:
   1) sprzęt komputerowy – serwer, komputery osobiste (w tym laptopy) i inne urządzenia zewnętrzne w tym urządzenia do monitoringu wizyjnego,
   2) oprogramowanie,
   3) dane osobowe zapisane na informatycznych nośnikach danych oraz dane przetwarzane w systemach informatycznych,
   4) hasła użytkowników,
   5) bazy danych i kopie zapasowe,
   6) wydruki,
   7) związana z przetwarzaniem danych dokumentacja papierowa.

2. Polityka bezpieczeństwa dotyczy przetwarzania wszystkich danych osobowych, przetwarzanych przez SKW w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, a także w systemach informatycznych będących w dyspozycji SKW i zawiera następujące informacje:
   A. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),
   B. rejestr czynności przetwarzania,
   C. sposób przepływu danych pomiędzy poszczególnymi systemami,
   D. środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
   E. procedury dotyczące postępowania w przypadku naruszenia danych osobowych

A. Obszar przetwarzania danych osobowych

Przetwarzanie danych osobowych przez SKW odbywa się zarówno przy wykorzystaniu systemów informatycznych jak i poza nimi, tj. w wersji tradycyjnej, „papierowej". Obszar przetwarzania danych osobowych przez SKW został określony w załączniku nr 1 do Polityki bezpieczeństwa pt.: „Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe". Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania danych osobowych.

B. Rejestr czynności przetwarzania

Dokument zawierający zestawienie zbiorów danych osobowych wraz z wskazaniem programów zastosowanych do przetwarzania danych oraz cele przetwarzania, kategorie odbiorców, opis kategorii osób których dane dotycząc wraz ze wskazaniem podstawy prawnej przetwarzania, stanowią załącznik 2 do Polityki bezpieczeństwa pt.: „Rejestr czynności przetwarzania".

C. Sposób przepływu danych pomiędzy poszczególnymi systemami.

W ramach procesów przetwarzania danych SKW nie dochodzi do przepływu danych pomiędzy różnymi systemami informatycznymi.

D. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Środki techniczne dotyczące systemów informatycznych zamieszczone zostały w instrukcji zarządzania systemami informatycznymi, stanowiącej załącznik nr 3 do Polityki bezpieczeństwa.

E. Procedury dotyczące postępowania w przypadku naruszenia danych osobowych.

Instrukcja postępowania w przypadku naruszenia danych osobowych stanowi załącznik nr 4 do Polityki bezpieczeństwa.

6. ELEMENTY I ŚRODKI ZABEZPIECZENIA DANYCH OSOBOWYCH.

1. Do elementów zabezpieczenia danych osobowych przez SKW zalicza się:
   1) stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe (zabezpieczenia fizyczne),

2) odpowiednie środki zabezpieczenia danych w systemach informatycznych (zabezpieczenia techniczne),
3) nadzór Administratora nad wprowadzonymi zasadami i procedurami zabezpieczenia danych (zabezpieczenie organizacyjne),
4) bezpieczeństwo osobowe.

2. **Zabezpieczenia fizyczne obejmują**:
   a) wydzielenie pomieszczeń i ich części, tworzących obszar przetwarzania danych,

W przypadku gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część w której przetwarzane są dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej.

Wydzielenie części pomieszczenia, w której przetwarzane są dane osobowe może być w szczególności dokonane przez montaż barierek, przegród lub odpowiednie ustawienie mebli biurowych uniemożliwiające lub co najmniej ograniczające niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.

   b) samodzielny dostęp do pomieszczeń jest możliwy wyłącznie dla osób upoważnionych, wstęp osób postronnych jest możliwy jedynie podczas obecności pracowników SKW posiadających stosowne upoważnienia,

W pomieszczeniach i częściach pomieszczeń, tworzących obszar przetwarzania danych SKW, mają prawo przebywać wyłącznie osoby upoważnione do dostępu i/lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania danych.

Osoby nieupoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać na obszarze przetwarzania danych wyłącznie w obecności upoważnionego pracownika SKW, lub w razie jego nieobecności, na podstawie upoważnienia wydanego, przez Administratora danych osobowych.

   c) zastosowanie środków zabezpieczających w przypadku czasowego lub całkowitego opuszczenia pomieszczenia.

Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejście osób niepowołanych.

Czasowe opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzania danych osobowych, obowiązany jest on umieścić zbiory występujące w formie papierowej w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym (w szczególności zablokowanie systemu operacyjnego komputera) uniemożliwiającym dostęp do danych osobowych osobom niepowołanym.

Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia budynku i/lub pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne i jako takie traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

d) kontrolę dostępu do pomieszczeń, w którym przetwarzane są dane,

Kontrola dostępu polegać będzie w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji uwzględnia się:

- imię i nazwisko osoby pobierającej lub zdającej klucz,
- numer lub inne oznaczenie pomieszczenia
- godzinę pobrania oraz zdania klucza

Klucze do pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do tych pomieszczeń na innych zasadach.

e) przechowywanie akt w wersji papierowej w specjalnie do tego celu przeznaczonych pomieszczeniach, w zamykanych na klucz szafach,

SKW zapewni aby w pomieszczeniach w których przetwarzane są dane osoby znajdowały się szafy zamykane na klucz, zapewniające bezpieczne przechowywanie danych w wersji papierowej. Ponadto w pomieszczeniach tych znajdować się urządzenia umożliwiające trwałe zniszczenie dokumentów zbędnych.

f) kopie zapasowe zbioru danych osobowych przechowywane są w sejfie winnym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

3. Zabezpieczenia techniczne obejmują:
   a) systemy informatyczne zastosowane do przetwarzania danych osobowych spełniają wymagania określone w Rozporządzeniu,
   b) w systemach informatycznych w Spółce obowiązują zabezpieczenia na poziomie wysokim, zgodnie z załącznikiem do Rozporządzenia,
   c) zastosowano mechanizmy kontroli dostępu do systemów informatycznych i ich zasobów; uprawnienia są różne dla różnych grup użytkowników,
   d) zastosowano odpowiednie i regularnie aktualizowane narzędzia ochronne, w tym oprogramowanie antywirusowe, które jest regularnie aktualizowane,
   e) system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
   f) tworzone są regularnie kopie zapasowe zbiorów danych przetwarzanych w systemach informatycznych oraz kopie programów służących do przetwarzania danych osobowych,
   g) zastosowano zabezpieczenia systemu przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (listwy przeciwzakłóceniowe),

4. **Zabezpieczenia organizacyjne** obejmują:
   a) pracownicy SKW, którzy na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą, o zaobserwowanych nieprawidłowościach informują Administratora;
   b) osoby upoważnione do przetwarzania danych osobowych mające dostęp do danych osobowych, które są w dyspozycji SKW, zobowiązane są do utrzymywania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu z określonego

stanowiska, a także po ustaniu zatrudnienia; w tym celu osoby te podpisują oświadczenie o utrzymywaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia,

Osoby upoważnione do przetwarzania danych osobowych zostaną zaznajomione z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi a także technikami i środkami ochrony tych danych. W szczególności osoby te zaznajamiane są tymi przepisami przed dopuszczeniem do pracy na stanowiskach związanych z przetwarzaniem danych, a w trakcie trwania zatrudnienia – w przypadku zmian tych przepisów, uregulowań lub technik i środków ochrony.

Zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony danych stosowanymi w SKW może odbywać się w szczególności poprzez:

- instruktaż na stanowisku pracy,
- szkolenie wewnętrzne,
- szkolenie zewnętrzne

Osoby przetwarzające dane osobowe SKW zostaną ponadto zaznajomione z zakresem informacji objętych tajemnicą w związku z wykonywaną przez siebie pracą, a w szczególności zostaną poinformowane o powinności zachowania w tajemnicy danych osobowych oraz sposobach ich zabezpieczenia.

Naruszenie przez zatrudnione w ramach stosunku pracy osoby upoważnione do dostępu i/lub przetwarzania danych osobowych, zasad bezpiecznego i zgodnego z prawem ich przetwarzania, traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

c) przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które zostały upoważnione do przetwarzania danych osobowych,

SKW dopuszcza do przetwarzania danych osobowych w systemie informatycznym i/lub tradycyjnym wyłącznie osoby posiadające upoważnienie nadane przez administratora danych osobowych lub inną upoważnioną do tego osobę.

d) kontrola nad dostępem do danych osobowych

Osoby przetwarzające dane osobowe zostały upoważnione do przetwarzania danych osobowych poprzez wpisanie określonych kompetencji do zakresu obowiązków na danym stanowisku.

5. W ramach **zabezpieczeń osobowych SKW**:
   a) stosować będzie klauzulę o zachowaniu poufności danych osobowych w umowach o pracę oraz w umowach ze zleceniobiorcami, z którymi związane jest przetwarzanie danych osobowych;
   b) wprowadzi się obowiązek raportowania do Administratora wszelkich naruszeń (incydentów), zauważonych podatności i innych słabych punktów oraz przypadków błędnego działania sprzętu i oprogramowania.

8. ROZPOWSZECHNIANIE I ZARZĄDZANIE DOKUMENTEM POLITYKI

1. Niniejszy dokument zawiera informacje o zabezpieczeniach, dlatego też został objęty ochroną na zasadzie tajemnicy przedsiębiorstwa w myśl art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.). Wybrane jego elementy mogą zostać udostępnione innym podmiotom po zawarciu stosownej umowy o zachowaniu poufności.
2. Za zarządzanie dokumentem Polityki Bezpieczeństwa, w tym jego rozpowszechnianiem, aktualizacją, utrzymywaniem spójności z innymi dokumentami, jest odpowiedzialny administrator danych.
3. Z treścią niniejszego dokumentu powinny zostać zapoznane wszystkie osoby upoważnione do przetwarzania danych osobowych, które z racji wykonywanych obowiązków i czynności mają dostęp do danych osobowych.
4. Integralną część niniejszej Polityki Bezpieczeństwa stanowią następujące załączniki:
   a) Załącznik nr 1 – Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe;
   b) Załącznik nr 2 – Rejestr czynności przetwarzania;
   c) Załącznik nr 3 – Instrukcja zarządzania systemem informatycznym
   d) Załącznik nr 4 – Instrukcja postępowania w sytuacji naruszenia danych osobowych
   e) Załącznik nr 5 – Wzór upoważnienia do przetwarzania danych osobowych;
   f) Załącznik nr 6 – Ewidencja osób upoważnionych do przetwarzania danych osobowych.