POLITYKA OCHRONY DANYCH OSOBOWYCH

Zakład Oczyszczania Miasta Sp. z o.o.

Centrala:
ul. Metalowców 4, 58-100 Świdnica

Oddział:
ul. Jasna 2A, 88-400 Żnin

maj 2018 r.

SPIS TREŚCI

ROZDZIAŁ I - CEL I ZAKRES

1) Administratorem danych osobowych jest Przedsiębiorstwo Recyklingu Odpadów i Przetwarzania Sp. z o.o. zwane w dalszej części „ZOM Sp. z o.o.”.
2) Celem Polityki Ochrony Danych Osobowych jest stworzenie podstawy dla metod zarządzania, procedur i wymagań niezbędnych dla zapewnienia w ZOM Sp. z o.o. właściwej ochrony informacji. Polityka Ochrony Danych określa w sposób szczegółowy zasady ochrony informacji w organizacji, niezależnie od systemów ich przetwarzania (zautomatyzowany, inny niż zautomatyzowany) oraz sposobu ich przetwarzania w tych systemach. Obejmuje bezpieczeństwo fizyczne, logiczne oraz komunikacyjne przetwarzanych informacji. Swoim zasięgiem obejmuje zarówno sprzęt i oprogramowanie, za pomocą których informacje są przetwarzane, jak i osoby które te informacje przetwarzają.
3) Polityka ma zastosowanie w stosunku do wszystkich pracowników, osób zatrudnionych na podstawie kontraktu menadżerskiego, konsultantów, stażystów i innych współpracowników ZOM Sp. z o.o., jak również pozostałych osób mających dostęp do informacji w Spółce. W dalszej części dokumentu pojęcie „Użytkownik” będzie używane dla wspólnego określenia powyższych kategorii.
4) Polityka Ochrony Danych Osobowych ma zastosowanie do wszelkich danych osobowych we wszystkich postaciach przetwarzanych w systemach informatycznych i komunikacyjnych przez ZOM Sp. z o.o.
5) Polityka Ochrony Danych Osobowych jest dokumentem przewidzianym w art. 24 ust. 2 Ogólnego Rozporządzenia 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 (Dz. U. UE. L. 2016.119.1, dalej jako RODO). Wdrożenie Polityki jest proporcjonalne i niezbędne do czynności przetwarzania realizowanych przez Spółkę.
6) Polityka Ochrony Danych w sposób szczegółowy opisuje wdrożone przez Spółkę techniczne i organizacyjne środki bezpieczeństwa danych osobowych, o których mowa w art. 32 ust. 1 RODO.
7) Polityka i Rejestr Czynności Przetwarzania muszą zawierać tożsame opisy procesów przetwarzania danych osobowych w Spółce.

ROZDZIAŁ II - OGÓLNE ZASADY

1) ZOM Sp. z o.o. przetwarza dane osobowe jako „administrator”.
2) ZOM Sp. z o.o. wdraża środki techniczne i organizacyjne ujęte w Polityce celem zapobieżenia naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (w tym przed: nieautoryzowanym dostępem, ujawnieniem, powielaniem, modyfikacją, zniszczeniem, utratą, zatajeniem, nieprawidłowym wykorzystaniem, kradzieżą).
3) Zakresem działalności ZOM Sp. z o.o. jest odbiór odpadów komunalnych od mieszkańców i podmiotów gospodarczych a także organizowanie selektywnej zbiórki odpadów oraz prowadzenie Punktu Selektywnego Zbierania Odpadów.

Użyte w Polityce określenia oznaczają:

SYSTEM INFORMATYCZNY	zautomatyzowany system przetwarzania informacji gromadzonych w zbiorach danych Spółki, który dostarcza i rozprowadza informacje
BAZA DANYCH	zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych danych. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane
ZBIÓR DANYCH	uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie
USUWANIE DANYCH	rozumie się przez to brakowanie dokumentów zawierających dane osobowe lub ich anonimizację, to jest trwałe usunięcie zapisów uniemożliwiające zidentyfikowanie osoby fizycznej
PRZETWARZANIE DANYCH	operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie
DANE OSOBOWE	informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); 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
ADMINISTRATOR	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
INSPEKTOR OCHRONY DANYCH	wyznaczona osoba, do której zadań należy: - informowanie administratora, podmiotu przetwarzającego oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie; - monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty; - udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO; - współpraca z organem nadzorczym (PUODO); - pełnienie funkcji punktu kontaktowego dla organu nadzorczego (PUODO) w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
PODMIOT PRZETWARZAJĄCY	osoba fizyczną lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO	należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych, a także ich utratą (poufność, integralność rozliczalność).
ZGODA OSOBY, KTÓREJ DANE DOTYCZĄ	rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie, zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
OSOBY UPOWAŻNIONE (UŻYTKOWNICY)	osoby wyznaczone przez Administratora upoważnione do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, które posiadają ustalony identyfikator oraz hasło, uprawnione do dostępu do danych osobowych
PRACOWNIK OCHRONY	osoba wykonująca zadania ochrony na rzecz ZOM Sp. z o.o.
KOMÓRKA ORGANIZACYJNA	każda komórka wydzielona organizacyjnie i funkcjonalnie, zgodnie z regulaminem organizacyjnym każdego podmiotu przetwarzającego dane osobowe

ROZDZIAŁ III - PODZIAŁ INFORMACJI – DANE OSOBOWE

1) Informacja – wszelka reprezentacja w świecie fizycznym informacji (w tym na papierze, nośnikach elektronicznych, zapisów bitów w pamięci urządzeń elektronicznych).
2) Ochronie podlega informacja o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (dane osobowe).
3) Wszystkie dane osobowe ZOM Sp. z o.o. to **dane ogólne i dane szczególne.**
4) Dane osobowe podlegają ochronie przed kradzieżą, nieautoryzowanym dostępem, modyfikacją, zatajeniem oraz utratą (zniszczeniem).
5) Inspektor Ochrony Danych stale nadzoruje prawidłowość przetwarzania danych osobowych w kategoriach wskazanych w punkcie 3).

ROZDZIAŁ IV OBOWIĄZKI UŻYTKOWNIKÓW

1) Obowiązek ochrony danych osobowych przetwarzanych w Spółce, a w szczególności zachowanie ich poufności i integralności obowiązuje każdą osobę, która ma dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w Spółce, bez względu na zajmowane stanowisko i miejsce wykonywania jak również podstawę prawną wykonywanych czynności (stosunek pracy, umowy cywilnoprawne, w tym biznes to biznes lub kontakt menadżerski) – Użytkownicy.
2) Każdy Użytkownik, który uzyskał dostęp do danych osobowych przetwarzanych przez Spółkę jest zobligowany do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom trzecim.
3) Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy, jak i po jego ustaniu, jak również podczas trwania stosunku współpracy, jak i po jej ustaniu.
4) Każdy Użytkownik, który uzyskał dostęp do danych osobowych przetwarzanych przez Spółkę jest osobiście odpowiedzialny za przestrzeganie zasad ochrony danych osobowych zawartych w niniejszym dokumencie.

ROZDZIAŁ V - DOSTĘP DO DANYCH OSOBOWYCH

1) Dostęp do danych osobowych w ZOM Sp. z o.o. oraz upoważnienie do ich przetwarzania przyznaje się Użytkownikowi w oparciu o funkcję jaką pełni w Spółce.
2) Funkcja jaką wypełnia dany Użytkownik związana jest z umową o pracę oraz zakresem jego obowiązków.
3) Czas dostępu do poszczególnych danych osobowych określony jest czasem wykonania zadania wynikającego
   z pełnionej funkcji.
4) Prawa dostępu do informacji zastrzeżonych nadaje Inspektor Ochrony Danych w porozumieniu z Administratorem.
5) Szczegóły nadawanie uprawnienia i polecenia przetwarzania danych określona jest w dalszej części przedmiotowej Polityki oraz w Polityce Zarządzania Systemem Teleinformatycznym.

ROZDZIAŁ VI - INSPEKTOR OCHRONY DANYCH I JEGO ZASTĘPCY

1) Inspektor Ochrony Danych wykonuje w imieniu ZOM sp. z o.o. zadania związane z ochroną danych osobowych w Spółce.
2) Inspektor Ochrony Danych decyduje o zasadach przetwarzania danych osobowych oraz o tym jakie osoby muszą mieć do nich dostęp.
3) Inspektor Ochrony Danych jest odpowiedzialny za ochronę danych osobowych. Kontroluje, w jakich systemach informacje z grupy są przetwarzane oraz jakie osoby i na jakich zasadach mają do nich dostęp.
4) Ponadto, do najważniejszych obowiązków Inspektora Ochrony Danych należy:
   a. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Inspektora Ochrony Danych;
   b. nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną oraz przestrzegania zasad w niej określonych;
   c. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   d. prowadzenie rejestru zbiorów danych przetwarzanych przez Administratora danych.
5) Inspektora Ochrony Danych ma prawo:
   a. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Spółce;
   b. wstępu do pomieszczeń w których zlokalizowane są zbiory danych po wcześniejszym ustaleniu tego ze Spółką i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z przepisami prawa;
   c. żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
   d. żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
   e. żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

ROZDZIAŁ VII – PRZETWARZANIE DANYCH OSOBOWYCH

1) Dane osobowe mogą być przetwarzane wyłącznie przy pomocy systemów, które spełniają warunki opisane w rozdziale Polityki *„Systemy przetwarzania danych osobowych”.*
2) Dane osobowe powinny być przechowywane wyłącznie przez czas niezbędny do ich eksploatacji.
3) Każda grupa danych osobowych musi posiadać przynajmniej jeden system do robienia kopii zapasowych (system wewnętrznej archiwizacji).
4) Korespondencję Spółki obsługuje jej Sekretariat.
5) W razie otrzymania przez Sekretariat Spółki danych osobowych, wobec których Spółka nie ma podstaw prawnych do przetwarzania, po zapoznaniu się z ich charakterem pracownik Sekretariatu natychmiast je anonimizuje lub je usuwa.

ROZDZIAŁ VIII – OSOBY UPOWAŻNIONE (UŻYTKOWNICY)

1) Użytkownikami są wszystkie osoby, które na podstawie pisemnego upoważnienia – osoby upoważnione - mogą przeglądać, edytować, tworzyć lub kasować dane osobowe.
2) Użytkownicy są zobowiązani zapoznać się i podpisać dokumenty dotyczące ochrony informacji w ZOM Sp. z o.o.
3) Prawa dostępu użytkownika do danej grupy danych osobowych ustala i kontroluje Inspektor Ochrony danych lub osoba przez niego pisemnie upoważniona.
4) Przez cały czas korzystania z danych osobowych, użytkownik jest kontrolowany przez Inspektora Ochrony Danych lub przez osobę przez niego wyznaczoną, systemy informatycznego do którego ma dostęp.
5) Użytkownik może stracić wszelkie prawa dostępu do tych danych osobowych na wniosek Inspektora Ochrony Danych w szczególności, gdy:
    a. dane nie będą jemu więcej potrzebne (zmieni się jego funkcja);
    b. naruszy Politykę Ochrony Danych Osobowych.

ROZDZIAŁ IX - SYSTEMY PRZETWARZANIA DANYCH OSOBOWYCH

1) Każdy system przetwarzania danych osobowych musi pozostawać pod stałym nadzorem Administratora lub osoby upoważnionej przez Administratora.
2) Każdy system przetwarzania danych osobowych musi być poddawany okresowo audytowi bezpieczeństwa.
3) Każdy system musi posiadać formalny opis procedur:
   a. *Zakładania kont użytkowników w systemie*;
   b. *Modyfikacji kont użytkowników w systemie* - awaryjnego odnawiania lub zmieniania atrybutów dostępu (np. zapomnianych haseł);
   c. *Usuwania kont użytkowników w systemie*.
4) Systemy, w których można przetwarzać dane osobowe muszą spełniać następujące warunki:
   a. **Kontrola** dostępu:
      i. System musi zapewniać, aby do danych będą miały dostęp wyłącznie upoważnione osoby;
      ii. System musi zapewniać, że upoważnione osoby będą mogły wykonywać wyłącznie dopuszczalne operacje;
      iii. System musi posiadać możliwość czasowego nadawania praw dostępu z automatycznym wygasaniem tych praw;
   b. **Integralność** - system musi się składać wyłącznie z dopuszczonych do systemu elementów i jego stan musi być pod kontrolą przez cały czas eksploatacji;
   c. **Jednoznaczność operacji** - system musi w jednoznaczny sposób umożliwiać identyfikację osób, które dokonały zmiany w danych osobowych;
   d. **Zarządzanie bezpieczeństwem** - system musi posiadać mechanizmy pozwalające wykryć próby nieautoryzowanego dostępu do danych lub przekroczenia przyznanych uprawnień w systemie;
   e. **Zarządzanie danymi osobowymi**:
      i. System musi zapewniać integralność danych osobowych przez cały czas przechowywania informacji;
      ii. System musi posiadać mechanizmy bezpowrotnego niszczenia danych osobowych.
5) Celem zabezpieczenia zbioru danych osobowych wprowadza się odpowiednie rozwiązania techniczne:

a. Stosuje się system izolacji i selekcji połączeń z siecią zewnętrzną (firewall), mechanizmy szyfrowania, systemy zasilania awaryjnego, programy antywirusowe i wykrywające szkodliwe oprogramowanie;
b. Dokonuje się kontroli przepływu informacji oraz kontroli działań inicjowanych z sieci publicznej oraz z wewnątrz sieci firmowej;
c. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych;
d. Każdy użytkownik systemu posiada unikalny identyfikator i korzysta z sobie tylko znanego hasła, systemu informatyczne rejestrują istotne pod względem ochrony danych osobowych działania użytkownika;
e. Każdy użytkownik posiada dostęp do systemu informatycznego o uprawnieniach adekwatnych do wykonywanych przez niego obowiązków, dostęp do danych jest możliwy wyłącznie po dokonaniu uwierzytelnienia za pomocą identyfikatora i hasła;
f. Wprowadza się ścisłą kontrolę dostępu do pomieszczeń serwerowni;
g. Tam, gdzie to możliwe wprowadza się kontrolę dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
h. Mechanizm zabezpieczenia i uwierzytelnienia użytkowników oraz procedury postępowania zostały szczegółowo opisane w Polityce Zarządzania Systemem Teleinformatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

6) Celem zabezpieczenia zbioru danych osobowych wprowadza się odpowiednie rozwiązania organizacyjne:
   a. Przetwarzania danych osobowych w Spółce może dokonywać wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych udzielone przez Spółkę jako administratora danych osobowych oraz przeszkolona w zakresie obowiązujących przepisów prawa oraz wewnętrznych procedur przetwarzania danych osobowych. Wzór upoważnienia i polecenia przetwarzania danych osobowych określa Załącznik nr 1. Wzór rejestru osób upoważnionych do przetwarzania danych osobowych określa Załącznik nr 2;
   b. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych;
   c. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych zgodnie z wymogami poufności i integralności. W szczególności w razie planowanej, choćby chwilowej, nieobecności Użytkownika obowiązany jest on umieścić zbiory występujące w

formach dokumentowych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiającym dostęp do danych osobowych jak i ich przetwarzanie osobom trzecim;

d. Użytkownik przyjmuje do wiadomości, że zdarzają się sytuacje, w których do utraty poufności danych dochodzi nie w wyniku ataku na system informatyczny – w tym złamania hasła i identyfikatora użytkownika, lecz w wyniku ich nieświadomego ujawnienia przez Użytkownika. Użytkownik przyjmuje do wiadomości, że w celu nieświadomego skłonienia go do ujawnienia hasła, loginu lub danych dotyczących systemu informatycznego może być on celem ataków socjotechnicznych ze strony osób trzecich. W związku z powyższym Użytkownik obowiązany jest zachować szczególną ostrożność przy komunikowaniu się oraz przyjmuje do wiadomości, że nie wolno mu ujawniać nadanego mu hasła ani loginu (identyfikatora) ani danych dotyczących systemu informatycznego jakimkolwiek osobom trzecim, jak i innym użytkownikom telefonicznie, listownie, w drodze listu elektronicznego (e-mail), odpowiedzi lub w jakikolwiek inny sposób;
e. Użytkownik systemu ponosi odpowiedzialność za wszystkie operacje na danych osobowych wykonane przy użyciu jego identyfikatora i hasła dostępu;
f. Opuszczenie przez Użytkownika obszaru ich przetwarzania bez zabezpieczenia budynku lub pomieszczenia oraz umiejscowionych w nim zbiorów danych przed dostępem osób trzecich jest niedopuszczalne;
g. Użytkownik jest obowiązany do uniemożliwienia osobom nieuprawnionym dostępu do danych osobowych przechowywanych w każdej postaci oraz do infrastruktury informatycznej Spółki. W szczególności dotyczy to wszelkich osób podających się za pracowników technicznych, serwisantów itp. W przypadku takich osób użytkownik obowiązany jest ze szczególną starannością do kontroli i potwierdzenia ich uprawnień, (np. posiadanego przez te osoby zlecenia) przed rozpoczęciem wykonywania przez nich działań. Niedozwolone jest pozostawianie takich osób bez nadzoru;
h. Zgodne z Polityką Zarządzania Systemem Teleinformatycznym wykonywane są kopie zapasowe danych.

7) Każda osoba, która zauważyła zdarzenie mogące być przyczyną lub mogące spowodować naruszenie bezpieczeństwa danych a w szczególności ich poufności i integralności, zobowiązana jest do natychmiastowego poinformowania Inspektora Ochrony Danych lub jego zastępców oraz swojego bezpośredniego przełożonego.
8) O naruszeniu bezpieczeństwa danych mogą świadczyć w szczególności takie sytuacje jak:
   a. Brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych;
   b. Brak możliwości zalogowania się przez Użytkownika pomimo użycia właściwego loginu i hasła;

c. Wykrycie na stanowisku komputerowym Użytkownika narzędzi programowych np. wirusów komputerowych, robaków, rootkit-ów, trojan-ów;
d. Stwierdzenie fizycznej ingerencji w stanowisko komputerowe Użytkownika;
e. Zamontowanie lub znajdowanie się na stanowisku komputerowym nowego, nieznanego urządzenia (narzędzi sprzętowych) np. przejściówki, w szczególności keyloggera sprzętowego, kamery, urządzeń podsłuchowych.

9) W sytuacjach opisanych w punkcie 8 lit. c lub d każdy Użytkownik obowiązany jest niezwłocznie zawiadomić o tym fakcie Inspektora Ochrony Danych lub jego zastępców, a także swojego bezpośredniego przełożonego .

ROZDZIAŁ X – SPRAWDZENIE SYSTEMU OCHRONY DANYCH OSOBOWYCH

1) Do sprawdzenia stanu ochrony danych osobowych upoważniony jest Inspektor Ochrony Danych oraz jego zastępcy, a także Spółka oraz wyznaczeni przez Administratora lub jego zastępców lub Spółkę kontrolerzy wewnętrzni lub zewnętrzni.
2) Sprawdzenie ma na celu weryfikację zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Sprawdzeniu podlegają stan faktyczny z zapisami Polityki Ochrony Danych Osobowych oraz Polityki Zarządzania Systemami Teleinformatycznymi, w szczególności: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami ustawy i aktów wykonawczych.
3) Inspektor Ochrony Danych lub jego zastępcy przygotowują plan sprawdzenia uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Plan sprawdzeń tworzony będzie na okres nie krótszy niż kwartał i nie dłuższy niż rok uwzględniając wymóg by każdy zbiór danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych były objęte sprawdzeniem co najmniej raz na pięć lat.
4) Sprawdzenia są przeprowadzane jest na podstawie planu sprawdzeń stanowiącego Załącznik nr 6 do niniejszej Polityki.
5) Po dokonanej kontroli podmiot ją przeprowadzający przygotowuje i przekazuje Administratorowi sprawozdanie ze sprawdzenia stanowiące Załącznik nr 7 do Polityki Ochrony Danych Osobowych. Na jego podstawie inicjowane są działania korygujące lub zapobiegawcze.

ROZDZIAŁ XI– SZKOLENIA UŻYTKOWNIKÓW

1) Każdy Użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych zgodnie z nadawanym upoważnieniem.
2) Za przygotowanie i przeprowadzenie szkolenia odpowiada Inspektor Ochrony Danych lub jego zastępcy.
3) Zakres i forma szkolenia powinny obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz politykami obowiązującymi w Spółce z zakresu danych osobowych, a także o zobowiązaniu się do ich przestrzegania.
4) Szkolenie zostaje zakończone podpisaniem przez uczestnika Oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
5) Oświadczenie wskazane w ust. 4 powyżej, którego wzór określa Załącznik nr 1 do niniejszej Polityki Ochrony Danych Osobowych jest przechowywany w aktach osobowych Użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ XII – PROCEDURY SZCZEGÓŁOWE

1) Procedurę postępowania w razie telefonicznego żądania podania danych osobowych określa Załącznik nr 9 do niniejszej Polityki Ochrony Danych Osobowych.
2) Procedurę udzielania informacji o przetwarzanych danych osobowych osobie, która zgłosiła takie żądanie określa Załącznik nr 10 do niniejszej Polityki Ochrony Danych Osobowych.
3) Procedurę rozpoznawania pisemnego umotywowanego żądania zaprzestania przetwarzania danych osobowych określa Załącznik nr 11 do niniejszej Polityki Ochrony Danych Osobowych.
4) Procedurę udostępniania danych osobowych określa Załącznika nr 12 do niniejszej Polityki Ochrony Danych Osobowych.

ROZDZIAŁ XIII - KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

1) Inspektor Ochrony Danych sprawuje bezpośredni nadzór nad przestrzeganiem zasad ochrony danych osobowych przetwarzanych w systemie informatycznym, określonych w niniejszej Polityce.
2) Kontrola ma charakter okresowych, regularnych lub doraźnych planów sprawdzeń.
3) Z każdego sprawdzenia wykonany jest raport, którego wzór określa Załącznik nr 6.
4) W przypadku nieobecności Inspektor Ochrony Danych jego zadania wykonują osoby wyznaczone przez Inspektor Ochrony Danych.
5) W przypadku nagłej, nieprzewidzianej nieobecności Inspektora Ochrony Danych, osobę zastępującą Inspektora wyznacza Administrator spośród osób ujętych w wykazie.
6) Inspektor Ochrony Danych dokonuje osobiście lub przez osoby wyznaczone kontroli i oceny funkcjonowania mechanizmów zabezpieczeń i ochrony, w tym przestrzegania zasad postępowania z kluczami.
7) Kontrole, o których mowa powinny być dokonywane nie rzadziej, niż co 90 dni.
8) Przedmiotem kontroli, o których mowa powinno być w szczególności:
   a. funkcjonowanie zabezpieczeń systemowych;
   b. prawidłowość funkcjonowania mechanizmów uwierzytelniania użytkowników i kontroli dostępu do zbioru danych osobowych;
   c. funkcjonowanie zabezpieczeń fizycznych;
   d. zasady przechowywania kartoteki ewidencyjnej;
   e. zasady i sposoby likwidacji oraz archiwizowania kartoteki ewidencyjnej;
   f. zasady tworzenia kopii zapasowych;
   g. realizacja procedur wdrożonych przez Administratora (w zależności od zbioru danych osobowych) w zakresie ochrony danych osobowych.

ROZDZIAŁ XIV - POSTĘPOWANIE W PRZYPADKU NARUSZENIA I PODEJRZENIA NARUSZENIA ZABEZPIECZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

1) Naruszenie ochrony danych może być skutkiem:
   a. szkodliwego wpływu środowiska na system przetwarzania danych;
   b. zewnętrznych zdarzeń losowych;
   c. zamierzonych lub niezamierzonych czynności użytkowników systemów przetwarzania danych;
   d. nieuprawnionych działań osób nieupoważnionych do dostępu do danych.
2) Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane:
   a. niewłaściwe parametry środowiska takie jak temperatura, wilgotność dla pomieszczeń, w których przetwarzane są dane;
   b. sytuacja klęski żywiołowej (pożar, powódź, huragan);
   c. naruszenie lub próby naruszenia integralności systemu do przetwarzania danych (np. stan urządzenia wchodzącego w skład systemu wskazuje na zakłócenie jego pracy – brak dostępu do sieci czy awaria komputera, stan aplikacji wskazuje na obecność wirusa komputerowego);
   d. naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje (dodane, zmiana, usunięcie), zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych);
   e. wykorzystywanie nielegalnych aplikacji lub elementów nielegalnego oprogramowania;
   f. istotne zakłócenie toku pracy procedur zapewniających ochronę przetwarzania danych (np. brak wprowadzenia wymaganego dokumentu lub potwierdzenia takiej operacji), pojawienie się odpowiedniego komunikatu alarmowego z tych procedur (np. utrata dostępu do danych);
   g. otrzymanie informacji o naruszeniu ochrony danych (np. sygnał o nieautoryzowanym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu, stan przeglądanych danych wskazuje na ingerencję w strukturę zbioru);
   h. niedopełnienie obowiązku ochrony danych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, niezablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach, gdzie przetwarza się dane);
   i. nieuprawniony dostęp lub próba dostępu do pomieszczeń, gdzie przetwarza się dane;

j. nieuprawniony dostęp lub próba dostępu do systemu przetwarzania danych (np. nieuprawniona praca na koncie użytkownika, istnienie nieautoryzowanych kont dostępu do danych – pojawienie się nowych lub niezablokowanie czy usunięcie starych);

k. ujawnienie indywidualnych haseł dostępu do danych;

l. wykonanie nieuprawnionych kopii danych;

m. zmiana lub usunięcie danych zapisanych na kopiach bezpieczeństwa lub archiwalnych;

n. brak nośnika zawierającego dane (np. zaginięcie wydruku, kopii bezpieczeństwa, dyskietki czy dysku);

o. niewłaściwe niszczenie nośników zdanymi pozwalające na ich odczyt;

p. inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych w ZOM Sp. z o.o.

3) W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony danych osobowych, osoba zatrudniona przy ich przetwarzaniu bezzwłocznie powiadamia o tym fakcie Inspektora Ochrony Danych lub upoważnioną przez niego osobę.

4) Określony wyżej obowiązek ciąży również na pozostałych Użytkownikach. Postępowanie w przypadku naruszenia i podejrzenia naruszenia zabezpieczenia systemu ochrony danych osobowych ma odpowiednie zastosowanie do przypadków naruszenia bądź podejrzenia naruszenia ochrony danych osobowych gromadzonych w kartotece ewidencyjnej.

5) W przypadku awarii systemu informatycznego spowodowanej błędem programu lub użytkownika odpowiednie zastosowanie mają postanowienia Polityki Zarządzania Systemem Teleinformatycznym ZOM sp. z o.o.

6) W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób stosuje się zasady postępowania określone w Instrukcji Bezpieczeństwa Pożarowego, obowiązującej u administratora budynku.

7) Do czasu przybycia Inspektora Ochrony Danych lub upoważnionej przez niego osoby, użytkownik systemu:

a. powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów bądź dowodów;

b. zabezpiecza elementy systemu informatycznego przed dostępem osób trzecich;

c. podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych;

d. Postanowienia odpowiednie zastosowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony kartoteki ewidencyjnej.

8) Inspektor Ochrony Danych lub osoba przez niego upoważniona, po przybyciu na miejsce:
   a. ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane, stan urządzeń i zbioru danych oraz identyfikuje wielkość negatywnych następstw incydentu;
   b. wysłuchuje relacji osoby zatrudnionej przy przetwarzaniu danych, która dokonała powiadomienia;
   c. podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.
9) Inspektor Ochrony Danych lub upoważniona przez niego osoba sporządza z przebiegu zdarzenia raport,
   w którym zamieszcza w szczególności informacje o:
   a. godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane;
   b. sytuacji, jaką zastał;
   c. dacie i godzinie powiadomienia;
   d. podjętych działaniach i ich uzasadnieniu.
10) Kopia raportu przekazywana jest bezzwłocznie Administratorowi, a w przypadku, gdy raport sporządzony został przez osobę upoważnioną przez Inspektora Ochrony Danych, także Inspektorowi Ochrony Danych.
11) Inspektora Ochrony Danych lub osoby przez niego upoważnione podejmują kroki zmierzające do likwidacji naruszeń zabezpieczeń systemu i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
   a. w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu;
   b. relacjonuje Administratorowi przedsięwzięte czynności;
   c. o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia systemu, a w razie ich wprowadzenia zaznajamia z nimi osoby zatrudnione przy przetwarzaniu danych.
12) W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora dyscypliny pracy, Inspektor Ochrony Danych lub upoważniona przez niego osoba wnioskuje o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec sprawcy/sprawców.
13) Użytkownik, w sytuacji, o której mowa, może kontynuować pracę dopiero po otrzymaniu pozwolenia od Inspektora Ochrony Danych**.**
14) W przypadku zaginięcia komputera przenośnego lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem przenośnym niezwłocznie

powiadamia Inspektora Ochrony Danych lub upoważnioną przez niego osobę, a ponadto w przypadku kradzieży najbliższą jednostkę policji.

15) W sytuacji, o której mowa w ust. 1 Inspektor Ochrony Danych lub upoważniona przez niego osoba podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajścia, który powinna podpisać także osoba, której skradziono lub której zaginął sprzęt oraz powiadamia Administratora.
16) W przypadku kradzieży komputera przenośnego razem z nośnikiem magnetycznym Inspektora Ochrony Danych lub upoważniona przez niego osoba podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.
17) Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki i przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Kodeksie Pracy oraz wynikającą z Ustawy.

ROZDZIAŁ XV - PROCES POSTĘPOWANIA W PRZYPADKU USZKODZENIA ZBIORU DANYCH

1) Odtworzeniem danych zajmuje się Inspektor Ochrony Danych lub osoba przez niego upoważniona.
2) Odtworzenie następuję według kroków:
   a. zawieszenie uprawnień użytkowników i zakomunikowanie o czasowym zablokowaniu dostępu do zbioru danych;
   b. ustalenie źródła awarii i obszar uszkodzeń;
   c. podjęcie działań w celu usunięcia awarii i próby naprawy zbioru danych;
   d. sprawdzenie poprawności i spójności zbioru danych;
   e. podanie systemu procedurze testowania i dopiero po stwierdzeniu poprawności jego działania następuje przywrócenie uprawnień dla użytkowników i poinformowanie ich o możliwości bezpiecznego przetwarzania danych.
3) W przypadku stwierdzenia niespójności bądź utraty danych następuje ich odzysk z kopii bezpieczeństwa /zapasowych/.
4) Inspektor Ochrony Danych lub osoba przez niego upoważniona sporządza raport z przebiegu i wyniku odtworzenia danych, który przekazuje Administratorowi.

XVI - POLITYKA CZYSTEGO BIURKA

1. Każdy użytkownik przetwarzający dane osobowe, posiadający samodzielne stanowisko pracy, po zakończeniu pracy zobowiązany jest pozostawić miejsce pracy w czystości zapewniający brak możliwości dostępu osób nieuprawnionych do jakichkolwiek dokumentów zawierających dane osobowe.
2. Wszystkie dokumenty zawierające lub mogące zawierać dane osobowe, przed zakończeniem pracy, powinny być umieszczone w odpowiednim miejscu zabezpieczającym przed dostępem osób nieuprawnionych (szafka zamykana na klucz/pomieszczenie zamykane na klucz).

Politykę kluczy dostępowych do wskazanych w pkt. 2 miejsc, określi Inspektor Ochrony Danych w ramach regulacji wewnętrznej i dogodnych dla użytkowników zasad.

ROZDZIAŁ XVII – POSTANOWIENIA KOŃCOWE

1) Polityka Ochrony Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom trzecim w żadnej formie.
2) Zarząd Spółki lub Inspektor Ochrony Danych oraz jego zastępcy są obowiązani zapoznać z treścią Polityk Ochrony Danych, w tym przedmiotowej Polityki Ochrony Danych Osobowych każdego Użytkownika.
3) Inne osoby lub podmioty mogą zostać zapoznane z treścią Polityk Ochrony Danych w razie zaistnienia takiej konieczności, o czym decyduje Zarząd Spółki lub Inspektor Ochrony Danych.
4) Wszystkie regulacje dotyczące systemów informatycznych określone w Politykach Ochrony Danych dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
5) Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce Ochrony Danych Osobowych i pozostałych Politykach Danych Osobowych w ZOM sp. z o.o.
6) W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO oraz przepisów krajowych.

Wykaz załączników:

Załącznik nr 1	**Wzór upoważnienia i polecenia do przetwarzania danych osobowych wraz z załącznikiem do indywidualnego zakresu czynności pracownika zatrudnionego w ZOM Sp. z o.o.;**
Załącznik nr 2	**Rejestr osób upoważnionych do przetwarzania danych osobowych wraz z poza systemową ewidencją przekazywanych informacji;**
Załącznik nr 3	**Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;**
Załącznik nr 4	**Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania;**
Załącznik nr 5	**Opis struktury zbiorów danych i sposobu przepływu danych pomiędzy systemami;**
Załącznik nr 6	**Plan sprawdzeń;**
Załącznik nr 7	**Sprawozdanie ze sprawdzenia;**
Załącznik nr 8	**Oświadczenie o wzięciu udziału w szkoleniu;**
Załącznik nr 9	**Procedura postępowania w razie telefonicznego żądania podania danych osobowych;**
Załącznik nr 10	**Procedura udzielania informacji o przetwarzanych danych osobowych osobie, która zgłosiła takie żądanie;**
Załącznik nr 11	**Procedura rozpoznawania pisemnego umotywowanego żądania zaprzestania przetwarzania danych osobowych;**
Załącznik nr 12	**Procedura udostępniania danych osobowych;**
Załącznik nr 13	**Wykaz Identyfikatorów;**
Załącznik nr 14	**Procedura haseł IOD.**