I POSTANOWIENIA OGÓLNE

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych zawartych w OCTJ. Opisane reguły określają granice dopuszczalnego zachowania wszystkich osób mających do czynienia z przetwarzaniem danych osobowych.

Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom tradycyjnych oraz informatycznych.

Dokument „Polityka bezpieczeństwa ochrony danych osobowych" – zwany dalej „Polityką bezpieczeństwa" wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, przeznaczony do wglądu do osób do tego upoważnionych. polityka bezpieczeństwa obowiązuje wszystkie osoby pracujące przy przetwarzaniu danych osobowych w OCTJ.

Wykazywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa w danym rejestrze zbioru danych.

DEFINICJE

§ 1

OCTJ - Ogólnopolskie Centrum Techniki Jazdy s.c. Małgorzata Prątnicka, Elżbieta Wyszyńska.
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).
Dane osobowe – informacja dotycząca zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
Polityka bezpieczeństwa – rozumiana jako polityka bezpieczeństwa danych osobowych.
Administrator danych osobowych (ADO) – administratorem danych osobowych jest OCTJ.
Administrator Systemu Informatycznego (ASI) – osoba upoważniona przez OCTJ, odpowiedzialna za funkcjonowanie tego systemu oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie.
Koordynator ochrony danych (KOD) - osoba upoważniona przez ADO do koordynowania działań związanych z prawidłowością przebiegu procesu przetwarzania danych osobowych w OCTJ.
Identyfikator użytkownika – ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Przetwarzanie danych – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

SYSTEM PRZETWARZANIA DANYCH OSOBOWYCH

§ 2

W skład systemu przetwarzania danych osobowych wchodzą:
a) dokumentacja papierowa (korespondencja, dokumenty pracowników),
b) wydruki komputerowe,
c) urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji,
d) procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.

CELE
POLITYKI BEZPIECZEŃSTWA

§ 3

1) Celem opracowania dokumentu jest zdefiniowanie sposobu i zakresu przetwarzania danych osobowych przez OCTJ oraz użytych w tym celu środków. Dokument ten określa także wymagania jakie muszą zostać spełnione w zakresie dostępu do danych osobowych oraz sposoby zabezpieczania tych danych. Wszelkie działania podejmowane w zakresie przetwarzania danych osobowych muszą być zgodne z niniejszą Polityką bezpieczeństwa procesów przetwarzania danych osobowych.
2) Celem niniejszej Polityki bezpieczeństwa, jest wskazanie działań, jakie należy wykonać a także ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki w zakresie zabezpieczenia danych osobowych.
3) Polityka bezpieczeństwa w OCTJ ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:
   a) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone OCTJ,
   b) naruszeń przepisów prawa oraz innych regulacji,
   c) utraty lub obniżenia reputacji OCTJ,
   d) strat finansowych ponoszonych w wyniku nałożonych kar,
   e) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.
4) Wszelkie działania podejmowane w zakresie przetwarzania danych osobowych muszą być zgodne z niniejszą Polityką bezpieczeństwa.

ZAKRES STOSOWANIA
POLITYKI BEZPIECZEŃSTWA

§ 4

1) Polityka bezpieczeństwa ma zastosowanie w stosunku do wszystkich postaci informacji zawierających dane osobowe, w szczególności dokumentów papierowych oraz zapisów elektronicznych i innych, będących własnością OCTJ, jak również przetwarzanych w systemach informatycznych.
2) Polityka bezpieczeństwa ma zastosowanie w stosunku do wszystkich pracowników, jak również osób i podmiotów z którymi OCTJ zawarła umowy o charakterze cywilno-prawnym, umowy powierzenia przetwarzania danych osobowych, którzy mają dostęp do danych osobowych.
3) Ochrona danych osobowych wynikająca z Polityki bezpieczeństwa jest realizowana na każdym etapie przetwarzania informacji.

§ 5

1) Dane osobowe są przechowywane w pomieszczeniach biurowych w siedzibie OCTJ w Mławie przy ul. H. Sienkiewicza 30A oraz w pomieszczeniach biurowych na obiekcie szkoleniowym Ośrodka Doskonalenia Techniki Jazdy w miejscowości Stare Kosiny 50D.
2) Korzystanie z komputerów przenośnych jest ograniczone wyłącznie dla pracowników zatrudnionych na wyższych stanowiskach i wymaga indywidualnej pisemnej zgody ADO.
3) Dane osobowe przechowywane są na dyskach komputerów oraz innych nośnikach danych w wyznaczonych do tego pomieszczeniach, do których dostęp ma wyłącznie ADO oraz osoby upoważnione.
4) OCTJ przekazuje podmiotom zewnętrznym przetwarzanie danych osobowych w zakresie i na zasadach określonych w umowie powierzenia w związku z tym dane osobowe są przechowywane w pomieszczeniach podmiotów przetwarzających na zlecenie.

II. ŚRODKI TECHNICZNE I ORGANIZACYJNE STOSOWANE W PRZETWARZANIU DANYCH

ZASADY
FUNKCJONOWANIA POLITYKI BEZPIECZEŃSTWA

§ 6

1) W zakresie przetwarzania danych osobowych OCTJ zobowiązany jest dołożyć szczególnej staranności w celu ochrony interesu osób, których te dane dotyczą, a w szczególności przestrzegać następujących zasad:
   a) zasady legalności – przetwarzać dane zgodnie z prawem;
   b) zasady celowości – dane zbierać tylko do oznaczonych, zgodnych z prawem celów i nie poddawać ich dalszemu przetwarzaniu niezgodnemu z tymi celami;
   c) zasady merytorycznej poprawności – dane muszą być zgodne z prawdą, pełne (kompletne) i aktualne;
   d) zasady adekwatności danych – przetwarzać tylko te dane, które są niezbędne ze względu na cel ich zbierania;
   e) zasada ograniczenia czasowego – przechowywać dane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania, tj. realizacji usługi lub/i wywiązywania się z zapisów umowy.
2) OCTJ Realizując Politykę bezpieczeństwa zapewnia, że dane osobowe przez cały okres przetwarzania zachowają następujące atrybuty:
   a) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
   b) integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
   c) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
   d) rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,
   e) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
   f) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
   g) niezawodność – zamierzone zachowania i skutki są spójne.
3) OCTJ realizując Politykę bezpieczeństwa dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   c) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
   d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

KOMPETENCJE I ODPOWIEDZIALNOŚĆ
W ZARZĄDZANIU BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

§ 7

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezgodny z RODO grozi wyciągnięcie odpowiedzialność przewidzianych przepisami prawa.

§ 8

Administrator danych osobowych (ADO):

a) formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
b) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
c) wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności oraz je odwołuje**,**
d) odpowiada za zgodne z prawem przetwarzanie danych osobowych,
e) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych **(Zał. nr 6)**,
f) prowadzi ewidencję zawartych umów powierzenia przetwarzania danych osobowych **(Zał. nr 7)**,
g) prowadzi ewidencję czynności przetwarzania danych osobowych **(Zał. nr 8)**,
h) prowadzi ewidencję zbiorów danych osobowych,
i) określa potrzeby w zakresie stosowanych zabezpieczeń,
j) udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
k) prowadzi szkolenia oraz bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe i zapewnia odpowiedni poziom przeszkolenia,
l) sprawuje nadzór nad bezpieczeństwem przetwarzania danych osobowych.

§ 9

Koordynator ochrony danych (KOD) – osoba wyznaczona przez OCTJ:

a) upoważniona do podpisywania stosownych dokumentów w zakresie ochrony danych osobowych m.in. upoważnień imiennych oraz umów powierzenia,
b) sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
c) nadzoruje opracowanie i aktualizowanie dokumentacji opisującej sposób przetwarzania danych oraz zastosowanych środków technicznych i administracyjnych zapewniających odpowiednią ochronę danych osobowych
d) nadzoruje przestrzeganie zasad określonych w dokumentacji,
e) zapewnia zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
f) prowadzi szkolenia pracowników upoważnionych do przetwarzania danych osobowych w zakresie ochrony tych danych.

§ 10

Administrator systemu informatycznego (ASI) – osoba wyznaczona przez OCTJ:

a) zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa,
b) doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
c) przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
d) nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
e) zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
f) prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

§ 11

Pracownik przetwarzający dane (PPD) – pracownik upoważniony przez OCTJ:

a) chroni prawo do prywatności osób fizycznych powierzających swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym,
b) zapoznaje się zasadami określonymi w Polityce bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym i składa oświadczenie o znajomości tych przepisów.

NADZÓR NAD BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

§ 12

W celu zapewnienia bezpieczeństwa danych osobowych ADO podejmuje niezbędne działania, polegające w szczególności na:

a) zapewnieniu kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
b) sprawowaniu nadzoru nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób,
c) wdrożeniu awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
d) sprawowaniu nadzoru nad tym, w jaki sposób odbywają się naprawy, konserwacja oraz likwidacja urządzeń komputerowych, na których zapisane są dane osobowe,
e) sprawowaniu nadzoru nad przydziałem haseł,
f) sprawowaniu nadzoru nad sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
g) sprawowaniu nadzoru nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
h) sprawowaniu nadzoru nad przeglądami, konserwacjami oraz uaktualnieniami systemów informatycznych oraz wszystkimi innymi czynnościami wykonywanymi na zdefiniowanych zbiorach danych osobowych,
i) sprawowaniu nadzoru nad obiegiem oraz przechowywaniem dokumentów i wydruków zawierających dane osobowe generowane przez system informatyczny,
j) sprawowaniu nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym oraz kontrolą dostępu do danych osobowych,
k) sprawowaniu nadzoru, aby dostęp osób, które utraciły uprawnienia do przetwarzania danych osobowych został natychmiast unieważniony poprzez właściwe zablokowanie konta umożliwiającego dostęp do danych osobowych,
l) podjęciu działań zmierzających do tego, aby jeżeli istnieją odpowiednie możliwości techniczne, na komputerach po upływie określonego czasu nieaktywności użytkownika uruchamiał się tzw. wygaszać ekranu, skonfigurowany w taki sposób żaby wznowienie pracy na komputerze było możliwe dopiero po podaniu właściwych danych uwierzytelniających,
m) sprawowaniu nadzoru, aby w pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych były ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane,

ZBIORY DANYCH OSOBOWYCH
PRZETWARZANE PRZEZ OCTJ

§ 13

1) Dane osobowe przetwarzane są w funkcjonalnie podzielonych bazach danych osobowych tzw. „Zbiorach danych osobowych" opisanych szczegółowo w ewidencji czynności przetwarzania danych osobowych.
2) Dane osobowe pozyskiwane są od osób, których dane dotyczą drogą ustną, pisemną, korespondencji elektronicznej (e-mail) lub telefoniczną.
3) OCTJ wyklucza możliwość zakupu a w szczególności sprzedaży podmiotom zewnętrznym danych osobowych zgromadzonych w określonych poniżej zabiorach.
4) OCTJ przetwarza dane osobowe zlokalizowane w nast. Zbiorach danych osobowych:
   a) zbiór danych klientów – dane osób biorących udział w szkoleniach,
   b) zbiór danych pracowników – dane osób związane z ich zatrudnieniem,
   c) zbiór danych w księdze korespondencji - dane osobowe zgromadzonych w księdze korespondencji wychodzącej.

SZKOLENIA PRACOWNIKÓW
UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 14

1) W OCTJ obowiązuje program szkolenia pracowników upoważnionych do przetwarzania danych osobowych w zakresie ochrony tych danych.
2) OCTJ realizując Politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia zaznajomienie osób posiadających upoważnienie do przetwarzania danych z powszechnie obowiązującymi przepisami prawa, procedurami wewnętrznymi, technikami i środkami ochrony tych danych.
3) Instruktażu prowadzi ADO, KOD bądź inna osoba do tego upoważniona. Potwierdzeniem odbycia szkolenia jest podpisanie stosownego *oświadczenia* **(Zał. nr 1)** po zapoznaniu się z *kartą instruktarzu wstępnego* z zakresu ochrony danych osobowych **(Zał. nr 2)**.
4) Osoba przeszkolona w zakresie zasad i sposobu realizacji ochrony danych osobowych podpisuje odpowiednie oświadczenie o zaznajomieniu się z obowiązującymi zasadami ochrony danych osobowych i zobowiązaniu do przestrzegania zasad dotyczących ochrony danych, zachowania w tajemnicy danych osobowych, do których ma dostęp oraz informacji o stosowanych przez OCTJ środkach technicznych i organizacyjnych w zakresie ochrony danych osobowych.

ZASADY UDZIELANIA DOSTĘPU
DO DANYCH OSOBOWYCH

§ 15

1) Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami RODO oraz zasadami zawartymi w obowiązującej Polityce bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu.
2) Dostęp do danych udostępniany jest na podstawie upoważnienia nadanego pracownikowi przez ADO.
3) W przypadku osób przetwarzających dane w systemie informatycznym na podstawie polecenia ADO udostępnione zostają dane umożliwiające uwierzytelnienie.
4) Dostęp do danych, przyznawanie, modyfikacja, wycofanie uprawnień odbywa się zgodnie z procedurą określoną w Instrukcji określającej sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 16

1) Dane osobowe mogą być przetwarzane wyłącznie przez osobę upoważnioną, czyli osobę posiadającą pisemne upoważnienie do przetwarzania, w którym ustala się zakres czynności, do wykonywania, których jest uprawniona oraz, w którym zobowiązuje się ją do zachowania poufności informacji pozyskanych w związku z przetwarzaniem danych oraz zastosowanych zabezpieczeń.
2) ADO wydaje pisemne *upoważnienie* do przetwarzania danych **(Zał. nr 3)**.
3) Z chwilą ustania stosunku pracy wygasają uprawnienia do przetwarzania danych osobowych osobom, którym upoważnienia zostały wydane.
4) Nie jest wymagane wystawienie dokumentu odwołującego upoważnienie do przetwarzania danych osobowych, z wyjątkiem sytuacji, gdy zmienia się zakres wcześniej przyznanego upoważnienia.

UDOSTĘPNIANIE DANYCH OSOBOWYCH INNYM PODMIOTOMI

§ 17

1) Dane osobowe mogą być udostępnione osobom lub podmiotom z mocy przepisów prawa lub w przypadku wiarygodnego uzasadnia potrzeby ich posiadania,
2) ADO wraz z KOD każdorazowo rozpatrują poprawność podstawy prawnej oraz celowość uzasadnienia i podejmują decyzję o udostępnieniu danych osobowych.
3) Decyzja podejmowana jest ze szczególnym uwzględnieniem ryzyka związanego z ewentualnym naruszeniem praw i wolności osób, których dane dotyczą.
4) ADO może korzystać z usług podmiotów specjalizujących się w ochronie danych osobowych w celu podjęcia właściwej decyzji dotyczącej udostępnienia danych osobowych.
5) Udostępnienie danych może nastąpić na pisemny wniosek zawierający:
   a) adresat wniosku (ADO),
   b) wnioskodawca,
   c) podstawa prawna (wskazanie potrzeby),
   d) wskazanie przeznaczenia,
   e) zakres informacji.
6) ADO odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

§ 18

1) Powierzenie danych może nastąpić wyłącznie w drodze pisemnej *umowy powierzenia przetwarzania* danych osobowych **(Zał. nr 4)**, w której osoba lub podmiot przyjmując dane zobowiązują się do przestrzegania obowiązujących przepisów RODO. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.
2) Podmiot przetwarzający dane na podstawie umowy o powierzeniu przetwarzania, jest uprawniony do przetwarzania danych w zakresie i celu określonym w treści umowy.
3) Jeżeli przetwarzanie danych osobowych zostało powierzone osobie trzeciej (firmie zewnętrznej), zgodnie z treścią zawartej w tym zakresie umowy, dane osobowe znajdują się w miejscu prowadzenia działalności przez podmiot przetwarzający na zlecenie.

PRAWA OSÓB KTÓRYCH DANE DOTYCZĄ

§ 19

1) Każda osoba fizyczna, której dane przetwarzane są w OCTJ ma prawo:
   a) zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych,
   b) do kontroli i poprawiania swoich danych osobowych,
   c) wniesienia umotywowanego żądania zaprzestania przetwarzania.
2) Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ADO, udzielając informacji o zawartości zbioru danych na piśmie.
3) Na ADO spoczywa obowiązek pisemnego poinformowania osoby tzw. *obowiązek informacyjny* **(Zał. nr 5)**, o jej prawach, kto jest jej ADO oraz w jakim celu pobrane dane będą wykorzystywane.
4) Ponadto każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
   a) ustalenia administratora danych, adresu jego siedziby i pełnej nazwy oraz danych kontaktowych,
   b) uzyskania informacji o podstawie prawnej przetwarzania danych i przewidywanym czasie ich przetwarzania,
   c) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
   d) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
   e) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej,
   f) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
   g) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem zasad określonych przez RODO albo są już zbędne do realizacji celu, dla którego zostały zebrane.
5) Prawo do bycia zapomnianym nie jest realizowane, gdy przepisy prawa zobowiązują OCTJ do przechowywania danych.

ZASADY DOSTĘPU ORAZ BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH OSOBOWYCH W FORMIE TRADYCYJNEJ

§ 20

1) Dane w rejestrach papierowych przetwarzane w sposób tradycyjny przechowuje się w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, w zamkniętych pomieszczeniach, szafach lub archiwach.
2) W pomieszczeniach tworzących obszar przetwarzania danych osobowych mają prawo przebywać wyłącznie osoby upoważnione do dostępu lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania tych danych.
3) 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 w budynkach, pomieszczeniach, bądź w częściach pomieszczeń, gdzie przetwarzane są dane

osobowe, wyłącznie w obecności upoważnionego pracownika lub na podstawie upoważnienia wydanego przez ADO.

4) Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca.
5) Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.
6) Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.
7) Dokumentację papierową należy:
   a) poukładać i posegregować,
   b) zabezpieczyć przed dostępem osób nieuprawionych,
   c) przechowywać w miejscu suchym, aby nie uległa zniszczeniu z powodu wilgoci.
   d) chronić przed kurzem, pleśnią, owadami oraz gryzoniami, itp.
   e) chronić przed silnym promieniowaniem UV mogącym doprowadzić do jej nieczytelności,
8) Wydruk takich dokumentów powinien być nadzorowany w sposób pozwalający dbać o ochronę danych zawartych na wydruku.
9) Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne i jako takie traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
10) Szczegółowe zasady dotyczące zabezpieczenia pomieszczeń oraz udostępniania kluczy do pomieszczeń, w których przetwarzane są dane osobowe określa Instrukcja postepowania z kluczami i zabezpieczenia pomieszczeń obowiązująca w OCTJ.

ZASADY DOSTĘPU ORAZ BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

§ 21

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w Instrukcji Zarządzania Systemem Informatycznym, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego w OCTJ.

III. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

NADAWANIE I REJESTROWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM

§ 22

1) Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.
2) Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ASI.
3) ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez ADO.
4) Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.
5) Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

ZABEZPIECZENIE DANYCH W SYSTEMIE INFORMATYCZNYM

§ 23

1) Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wykonywana manualnie przez ASI.
2) W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.
3) System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
   a) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
   b) operacje wykonywane na przetwarzanych danych,
   c) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
   d) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
   e) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
4) System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem: identyfikatora osoby, której dane dotyczą, osoby przesyłającej dane, odbiorcy danych, zakresu przekazanych danych osobowych, daty operacji, sposobu przekazania danych.

§ 24

1) Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania") na każdym komputerze, na którym przetwarzane są dane osobowe.
2) Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

ZASADY BEZPIECZEŃSTWA
PODCZAS PRACY W SYSTEMIE INFORMATYCZNYM

§ 25

1) W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
   a) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła,
   b) loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.
2) W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z sytemu lub uruchomienie wygaszacza ekranu chroniony hasłem.
3) W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4) Użytkownik przed wyłączeniem komputera powinien zamknięcie w bezpieczny sposób wszystkie programu przetwarzającego dane.
5) Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników OCTJ przez ASI na co najmniej 30 minut przed planowanym zawieszeniem.
6) Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI w razie:
   a) podejrzenia naruszenia bezpieczeństwa systemu,
   b) braku możliwości zalogowania się użytkownika na jego konto,
   c) stwierdzenia fizycznej ingerencji w przetwarzana dane,
   d) stwierdzenia użytkowania narzędzia programowego lub sprzętowego.
7) Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:
   a) nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem),
   b) wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, itp.,
   c) różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych),
   d) inne nadzwyczajne sytuacje.

TWORZENIE KOPII ZAPASOWYCH

§ 26

1) Pełne kopie zapasowe Zbiorów danych zapisywane są na serwerze co 24 godziny. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
2) Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest ASI lub upoważniony pracownik obsługujący dany program przetwarzający dane.
3) Kopie przechowywane są szafie metalowej w wyznaczonym pomieszczeniu na terenie OCTJ.
4) Kopie zapasowe Zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ASI lub upoważniony do tego pracownik.
5) Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny wg. *protokołu usuwania/niszczenia danych* **(Zał. nr 9)**

PRZEGLĄDY I KONSERWACJE SYSTEMÓW

§ 27

1) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez ASI lub przez upoważnionych przedstawicieli wykonawców.
2) Prace wymienione w pkt. 1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3) Wszystkie prace wykonywane przez ASI lub innych wykonawców, a szczególności te mogące wpłynąć na proces przetwarzania danych osobowych powinny być odpowiednio wcześniej zgłaszane do ADO.
4) Przed rozpoczęciem pracy przez osoby niebędące pracownikami OCTJ należy dokonać potwierdzenia tożsamości tychże osób.

NISZCZENIE WYDRUKÓW I NOŚNIKÓW DANYCH

§ 28

1) Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek w sposób uniemożliwiający ich odczytanie.
2) Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3) Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

IV. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

ISTOTA NARUSZENIA DANYCH OSOBOWYCH

§ 29

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

a) nieautoryzowany dostęp, modyfikacja lub zniszczenie danych,
b) udostępnienie danych nieautoryzowanym podmiotom,
c) nielegalne ujawnienie danych lub ich pozyskiwanie z nielegalnych źródeł.

POSTĘPOWANIE W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH

§ 30

1) Każdy pracownik OCTJ, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to do ADO.
2) Każdy pracownik OCTJ, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz w miarę możliwości ustalić przyczynę i sprawcę naruszenia ochrony.
3) W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.
4) ADO podejmuje następujące kroki:
   a) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy OCTJ,
   b) może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
   c) rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu właściwemu organowi ds. ochrony danych osobowych,
   d) jeśli sytuacja tego wymaga nawiązuje kontakt z zewnętrznymi specjalistami w celu dalszej konsultacji,
   e) w przypadku stwierdzenia, że naruszenie skutkuje ryzykiem naruszenia lub wolności osób fizycznych zgłasza incydent w ustawowym terminie (72 godzin po stwierdzeniu naruszenia) właściwemu ds. ochrony danych osobowych,
5) ADO dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport.
6) ADO ma obowiązek zgromadzenia wszelkiej dokumentacji związanej z incydentem naruszenia ochrony danych. W szczególności administrator danych ma obowiązek udokumentować i opisać:
   a) okoliczności naruszenia ochrony danych osobowych,
   b) skutki,
   c) podjęte działania zaradcze.
7) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia

osobę, której dane dotyczą, o takim naruszeniu, opisując charakter naruszenia ochrony danych osobowych oraz poinformować osobę, której dane zostały naruszone o:
   a) w jaki sposób można skontaktować się z administratorem danych w celu uzyskania dodatkowych informacji,
   b) opisać możliwe konsekwencje naruszenia ochrony danych,
   c) opisać zastosowane przez administratora danych środki w celu zminimalizowania skutków naruszenia ochrony oraz podjętych działaniach zmniejszających ryzyko naruszenia ochrony w przyszłości.
8) Zawiadomienie nie jest wymagane, w następujących przypadkach:
   a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   b) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku administrator danych wydaje publiczny komunikat, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
9) ADO zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

KONSEKWENCJE NARUSZENIA POLITYKI BEZPIECZEŃSTWA

§ 31

1) Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami w uzasadnionych przypadkach wszczyna się postępowanie dyscyplinarne.
2) Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z przewidzianymi przepisami prawa.
3) Za nieprzestrzeganie zasad bezpieczeństwa danych osobowych pracownik może być ukarany karą upomnienia, nagany, bądź karą pieniężną, na zasadach określonych w przepisach Kodeksu Pracy.
4) Jeżeli naruszenie zasad bezpieczeństwa danych osobowych wiąże się z naruszeniem przepisów prawa, pracownik ponosi odpowiedzialność w trybie i na zasadach określonych w tych przepisach.

V. INSTRUKCJA POSTEPOWANIA Z KLUCZAMI I ZABEZPIECZENIA POMIESZCZEŃ

POSTĘPOWANIE Z KLUCZAMI

§ 32

1) Dostęp do kluczy i kodów dostępu do budynku i pomieszczeń posiadają jedynie pracownicy którzy otrzymali pisemne upoważnienie od Administratora i podpisali stosowne oświadczenie **(Zał. nr 10)**.
2) Osoby upoważnione do posiadania kluczy oraz kodów dostępu do budynku i pomieszczeń, o których mowa w § 5 Polityki bezpieczeństwa to pracownicy OCTJ:
   a) Andrzej Prątnicki – kierownik OCTJ,
   b) Zbigniew Wyszyński – koordynator ds. szkoleń i ochrony danych,
   c) Ewelina Pietrzak – specjalista ds. administracyjno-kadrowych,
   d) Monika Rychłowska – pracownik biurowy.
   e) Alicja Słowikowska – pracownik sprzątający

   W dalszej części Instrukcji zwane :Pracownikiem upoważnionym".
3) Pracownik upoważniony o którym mowa w ust.1, e) posiada upoważnienie jedynie w zakresie dostępu do kluczy od budynku i pomieszczeń mieszczących się na obiekcie szkoleniowym ODTJ w miejscowości Stare Kosiny 50D.
4) Klucze, o których mowa w ust 1, Pracownicy upoważnieni posiadają przy sobie.
5) Klucze do szafek zamykanych na klucz, w których gromadzona jest i przechowywana dokumentacja związana z prowadzoną przez Firmę działalnościa po zakończeniu pracy przechowywane są w oddzielnie zamykanym miejscu w szafie pancernej, do której klucz i wyłączny dostęp posiada ADO oraz osoby o, których mowa w ust.2 z wyłączeniem pracowników o których mowa w ust.2 d,e).
6) Klucze zapasowe do pomieszczeń są przechowywane w opieczętowanych, indywidualnie oznakowanych pojemnikach w szafie pancernej zamkniętej na klucz w siedzibie firmy.
7) O utracie, uszkodzeniu lub zniszczeniu kluczy, Pracownik upoważniony powiadamia pisemnie ADO.

§ 33

1) Dorabianie kluczy do pomieszczeń i budynków, o których mowa w § 5 Polityki bezpieczeństwa wymaga pisemnej zgody ADO i jest dozwolone wyłącznie w celu zastąpienia kluczy utraconych, uszkodzonych lub zniszczonych.
2) Klucze zniszczone należy przechowywać lub usuwać w sposób uniemożliwiający wykorzystanie ich do nieuprawnionego dostępu do pomieszczeń.
3) Jeżeli z okoliczności udostępnienia klucza osobie nieupoważnionej lub jego utraty wynika, że może zostać wykorzystany do nieuprawnionego dostępu do pomieszczenia lub budynku, należy wymienić odpowiedni zamek lub jego elementy współpracujące z kluczem.
4) Od momentu pobrania kluczy do momentu ich zdania Administratorowi, na upoważnionej osobie spoczywa pełna odpowiedzialność za mienie znajdujące się w danym pomieszczeniu.

§ 34

Zabrania się:

a) udostępniania osobom nieupoważnionym kluczy i kodów dostępowych,
b) pozostawiania otwartych pomieszczeń lub kluczy bez dozoru,
c) pozostawiania otwartych okien po zakończeniu pracy.

ZABEZPIECZENIE POMIESZCZEŃ

§ 35

1) Przed wyjściem z pomieszczenia, Pracownicy zobowiązani są do:
   a) uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających, polegających na:
      – pochowaniu wszystkich dokumentów w przystosowanych do tego celu biurkach i szafkach oraz zamknięcie ich na klucz,
      – wyłączeniu wszystkich urządzeń zasilanych energią elektryczną, (grzejniki, czajniki, wentylatory itp.) zgodnie z zasadami BHP i PŻ,
      – wyłączeniu oświetlenia,
      – zamknięciu okien i drzwi wyjściowych,
      – włączeniu systemu alarmowego - jeżeli jest i działa.
2) Za zniszczenia i uchybienia wymienione w pkt. 1. odpowiada osoba, która wcześniej dysponowała kluczami.

§ 36

1) Za utrzymanie skutecznego zabezpieczenia wszystkich pomieszczeń odpowiada bezpośrednio Administratorowi.
2) Za nieprzestrzeganie niniejszej instrukcji osoba ponosi odpowiedzialność wynikającą z art. 363 § 1 Kodeksu cywilnego.

V. POSTANOWIENIA KOŃCOWE

§ 37

1) Polityka bezpieczeństwa jest regularnie przeglądana i aktualizowana w zależności od potrzeb wynikających ze zmiany przepisów w tym zakresie z uwzględnienie podejmowanych decyzji i zmian wprowadzanych w firmie.
2) Niniejsza Polityka bezpieczeństwa przyjęta została Uchwałą z dnia 12 marca 2018r. przez Wspólników a wchodzi w życie z dniem 25 maja 2018 roku.

.....
(podpis Wykonawcy)