POLITYKA BEZPIECZEŃSTWA INFORMACJIw ACCATA Sp. z o.o. z dnia 24.05.2018 r.

Niniejsza Polityka bezpieczeństwa, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w „ACCATA" sp. z o.o. w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).

Definicje:

1. **Administrator Danych Osobowych zwany dalej „ADO" lub zamiennie „Administrator"** – podmiot, który jest odpowiedzialny za nadzór nad przestrzeganiem zasad ochrony danych osobowych w jednostce; decyduje o celach i środkach przetwarzania danych osobowych; wykonuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym „ACCATA" sp. z o.o. z siedzibą w Warszawie przy ul. Bitwy Warszawskiej 1920 r. nr 19, dla której Sąd Rejonowy dla m.st. Warszawy XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000131628, NIP 522-26-69-663.
2. **analiza ryzyka** - proces mający na celu oszacowanie wagi ryzyka rozumianego, jako funkcja prawdopodobieństwa wystąpienia skutku i krytyczności jego następstw dla jednostki;
3. **bezpieczeństwo informacji** - stan, w którym informacja jest chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności, zminimalizować straty i maksymalizować zwrot nakładów na inwestycje. Niezależnie od tego, jaką formę informacja przybiera lub za pomocą jakich środków jest udostępniana lub przechowywana, zawsze powinna być w odpowiedni sposób chroniona, bezpieczeństwo informacji oznacza
w szczególności zachowanie: poufności, integralności, dostępności, rozliczalności;
4. **dane osobowe (dane)** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5. **hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
6. **identyfikator** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
7. **IZSI** - Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
8. **nośnik** - wszelkiego rodzaju fizyczne środki służące do zapisu danych, używane w procesie przetwarzania, w szczególności dyski twarde, płyty CD/DVD, taśmy do streamerów, pamięci przenośne, dyski magnetooptyczne, dokumenty w formie papierowej;
9. **ochrona** - zespół środków organizacyjno-technicznych i prawnych zapewniających bezpieczeństwo informacji;
10. **osoba upoważniona do przetwarzania danych osobowych** - osoba, która została upoważniona

do przetwarzania danych osobowych u Administratora przez Administratora współpracująca
z Administratorem na podstawie umowy o pracę/ umów o współpracy. W dalszej części Polityki do określenia osoby upoważnionej do przetwarzania danych osobowych używa się także nazwy zamiennej „użytkownik”;

11. **plik** - ciąg bajtów posiadający swoją nazwę odróżniającą ją od innych plików i parametry, rozmiar, datę powstania lub datę ostatniej modyfikacji itp.;
12. **przetwarzanie danych** - wykonywanie jakichkolwiek operacji na danych osobowych, np.: zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie i przechowywanie;
13. **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
14. **ryzyko** - prawdopodobieństwo tego, że zagrożenie wykorzysta podatność powodując skutek;
15. **system informatyczny (system)** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16. **uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
17. **wirus** - program, który uaktywniony w pamięci operacyjnej, powoduje wadliwe działanie, zniszczenie lub modyfikację systemu operacyjnego, programu komputerowego lub danych;
18. **zagrożenie** - stan faktyczny, który może spowodować naruszenie bezpieczeństwa informacji;
19. **zbiór danych** - zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów.

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych u Administratora niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Celem niniejszej Polityki jest stworzenie podstaw organizacyjnych dla wdrożenia systemu zarządzania bezpieczeństwem danych osobowych w jednostce oraz określenie podstawowych zasad i wymagań organizacyjno-technicznych oraz prawnych dla zapewnienia właściwej ochrony informacji.
3. W związku z tym, że system informatyczny posiada szerokopasmowe połączenie z Internetem, niniejsza polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.
4. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
5. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
6. Dane osobowe przetwarzane przez ADO, a uzyskane w związku z prowadzeniem działalności gospodarczej przez Administratora, w tym w szczególności w celu

zapewnienia bieżącej obsługi
w zakresie usług oferowanych przez Administratora.

7. Administrator zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.
8. Dla skutecznej realizacji zasad niniejszej Polityki Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
   b) kontrolę i nadzór nad przetwarzaniem danych osobowych,
   c) monitorowanie zastosowanych środków ochrony, które obejmuje monitorowanie przez Administratora zastosowanych środków ochrony obejmuje m.in. działania osób upoważnionych do przetwarzania danych osobowych, naruszanie zasad dostępu do danych osobowych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

II. Dane osobowe przetwarzane u Administratora.

1. Dane osobowe przetwarzane przez Administratora gromadzone są w zbiorach danych.
2. ADO nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób, których dane osobowe są przetwarzane. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania ADO dokonuje analizy ryzyka ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi **Załącznik nr 1** do niniejszej Polityki.
5. Przetwarzanie danych osobowych dopuszczalne jest wyłącznie na wyznaczonym do tego obszarze.
6. Dane osobowe w jednostce przetwarzane są w systemie informatycznym funkcjonującym
   w budynku **przy ul. Bitwy Warszawskiej 1920 r. nr 19.**
7. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych, stanowi Załącznik nr 2 do niniejszej Polityki.
8. W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), jednak wymaga to zgody indywidualnej ADO.
9. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych, wydane przez ADO.
10. Upoważnioną do przetwarzania danych może być tylko osoba, która uczestniczyła uprzednio
    w szkoleniu z zakresu ochrony danych osobowych.
11. Osoba posiadająca upoważnienie do przetwarzania danych jest uprawniona do ich przetwarzania
    w zakresie i czasie wskazanym w upoważnieniu.
12. Dostęp zatrudnionych osób do zasobów informacyjnych ograniczony jest zgodnie z zasadą wiedzy koniecznej.
13. Wzór upoważnienia do przetwarzania danych stanowi Załącznik nr 3 do niniejszej Polityki.

14. Wzór oświadczenia o zachowaniu poufności przetwarzanych danych stanowi Załącznik nr 4
    do niniejszej Polityki.
15. Rejestr osób upoważnionych do przetwarzania danych osobowych stanowi Załącznik nr 5
    do niniejszej Polityki.

III. Obowiązki i odpowiedzialność w zakresie zarzadzania bezpieczeństwem

1. Wszystkie osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym,
   a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych obowiązujących u ADO o ile takowe wdrożono.
2. Wszystkie dane osobowe są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
   a) W każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych osobowych.
   b) Dane osobowe są przetwarzane są rzetelnie i w sposób przejrzysty.
   c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach
      i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
   d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągniecia celu przetwarzania danych.
   e) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane.
   f) Czas przechowywania danych osobowych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.
   g) Dane osobowe są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Każdy osoba upoważniona do przetwarzania danych osobowych mająca dostęp do systemu informatycznego odpowiada za ochronę informacji przetwarzanych w systemie zgodnie
   z indywidualnym zakresem obowiązków, nadanymi uprawnieniami i zakresem odpowiedzialności wynikającym
   z zajmowanego stanowiska przez tę osobę.
4. Obowiązkiem każdej osoby upoważnionej do przetwarzania danych osobowych która jest jednocześnie użytkownikiem systemu informatycznego jest:
   a) przestrzeganie przepisów prawa i przepisów wewnętrznych jednostki;
   b) dbałość o zachowanie bezpieczeństwa informacji, do których ma dostęp;
   c) zgłaszanie do bezpośredniego przełożonego oraz ADO przypadków naruszenia bezpieczeństwa informacji.
   d) Stosowanie się do wskazówek wyszczególnionych w dziale II pkt. 20 niniejszej Polityki.
5. Fizyczną ochronę danych osobowych i ich przetwarzania realizuje się poprzez:
   a) przetwarzanie danych osobowych w ściśle określonych miejscach do tego przeznaczonych;
   b) zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe poprzez zastosowanie wysokiej jakości zamków drzwiowych, do których

klucze posiadają tylko uprawnione osoby;

c) zamykanie pomieszczeń, w których przetwarzane są dane osobowe na czas nieobecności
w nich osób upoważnionych do przetwarzania danych osobowych;

d) zabezpieczenie wszelkich możliwych dróg dostępu do pomieszczeń, w tym również okien;

e) wyposażenie pomieszczeń w sprzęty oraz meble biurowe dające gwarancję bezpieczeństwa dokumentacji (szafy, biurka zamykane na klucz);

f) zapewnienie odpowiedniej organizacji stanowisk pracy osobom, które przetwarzają dane osobowe;

g) dane osobowe po zakończeniu pracy przechowywane są w zamykanych na klucz meblach biurowych.

6. Techniczną ochronę danych i ich przetwarzania realizuje się poprzez:

a) zastosowanie wykonanych z materiałów nieprzezroczystych teczek oraz segregatorów,
w których przechowywane są dane osobowe;

b) oznaczenie teczek oraz segregatorów, w których przechowywane są dane osobowe w sposób utrudniający identyfikację ich zawartości osobom nieupoważnionym;

c) wykorzystywanie mechanizmów systemu operacyjnego, nadawanie uprawnień i praw dostępu;

d) komputer, z którego możliwy jest dostęp do danych osobowych, zabezpieczony jest hasłem dostępu;

e) zastosowanie wygaszaczy ekranu w przypadku nieaktywności jej użytkownika;

f) zastosowanie blokady hasłem podczas dłuższej nieaktywności użytkownika;

g) zastosowanie na komputerach użytkowników bazy danych programów antywirusowych;

h) wykonywanie kopii zapasowych przetwarzanych baz danych osobowych i zapisywane
na nośnikach danych osobowych.

7. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

a) może przetwarzać dane osobowe zgodnie z zakresem opisanym w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych osobowych przypisany jest do niepowtarzalnego identyfikatora nadanego osobie upoważnionej do przetwarzania danych osobowych, niezbędnego do rozpoczęcia pracy w systemie. Ustanie stosunku pracy/umowy o współpracy powoduje wygaśnięcie nadanego upoważnienia do przetwarzania danych osobowych;

b) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia, a także po ustaniu stosunku pracy/ umowy o współpracy;

c) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki i IZSI służącym do przetwarzania danych osobowych;

d) stosuje określone przez ADO procedury oraz wytyczne mające na celu zgodne z prawem,
w tym zwłaszcza adekwatne i celowe przetwarzanie danych osobowych;

e) korzysta z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;

f) zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym.

8. Osoba upoważniona do przetwarzania danych osobowych winna podejmować działania we własnym zakresie zmierzające do prawidłowego zapewnienia najskuteczniejszej ochrony danych osobowych, w tym w szczególności:

a) ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;

b) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych oraz w samochodach;

c) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);

d) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);

e) pilnego strzeżenia akt, pamięci przenośnych, nośników danych i komputerów przenośnych;

f) kasowania danych zgodnie z procedurą IZSI po wykorzystaniu danych osobowych na dyskach przenośnych;

g) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;

h) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;

i) zabrania się osobom upoważnionym do przetwarzania danych osobowych samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu;

j) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń Administratora;

k) opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej;

l) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych osobowych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez tego użytkownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne i przechowywane w zamkniętych na klucz szafach lub szufladach. Po ustaniu przydatności tych kopii dane osobowe należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;

m) udostępniania danych osobowych pocztą elektroniczną tylko po uzyskaniu pisemnej zgody osoby, której dotyczą;

n) niewynoszenia na jakichkolwiek nośnikach danych całych zbiorów danych osobowych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;

o) kończenia pracy na stacji roboczej po wprowadzeniu danych osobowych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika
i wyłączeniu komputera;

p) niszczenia w niszczarce lub chowania do szaf wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

q) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są

dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;

r) zachowania tajemnicy danych osobowych, w tym także wobec najbliższych;

s) chowania do szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

t) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;

u) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;

v) zamykania drzwi na klucz (blokowania kartą magnetyczną) przy każdym wyjściu z pomieszczenia oraz po zakończeniu pracy w danym dniu. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym pracowników sprzątających, celem uniknięcia zagubienia lub wyrzucenia dokumentów zawierających dane osobowe.

9. Organizacyjną ochronę danych osobowych i ich przetwarzania realizuje się poprzez:

a) zapoznanie każdej osoby upoważnionej do przetwarzania danych osobowych z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu;

b) przeszkolenie osób, o których mowa w pkt 1, w zakresie bezpiecznej obsługi urządzeń
i programów związanych z przetwarzaniem i ochroną danych osobowych oraz zabezpieczenia pomieszczeń i budynków;

c) odebranie od osób upoważnionych do przetwarzania danych osobowych oświadczeń
o zachowaniu poufności przetwarzanych danych osobowych;

d) identyfikatory oraz hasła dostępu do poszczególnych baz danych są jedynie w posiadaniu ADO, który jest zobowiązany do przechowywania ich w zamykanych na klucz meblach biurowych,
do których nie mają dostępu osoby nieupoważnione.

IV. Bezpieczeństwo sprzętu i oprogramowania

1. Sprzęt informatyczny i oprogramowanie podlega właściwej ochronie opisanej w IZSI. Treść IZSI stanowi Załącznik nr 6 do niniejszej Polityki.
2. Sprzęt informatyczny oraz oprogramowanie wykorzystywane w systemach informatycznych muszą być zgodne z przepisami prawa i powinny być zgodne z najlepszymi praktykami.
3. System informatyczny może składać się wyłącznie z przetestowanego, formalnie dopuszczonego do eksploatacji sprzętu i oprogramowania.
4. Sprzęt i oprogramowanie powinny być eksploatowane, serwisowane i wycofywane z eksploatacji
z zachowaniem właściwych procedur bezpieczeństwa.
5. Oprogramowanie instalowane w systemach informatycznych musi być legalne.
6. Wszelkie oprogramowanie musi być użytkowane z poszanowaniem praw własności intelektualnej,
a w szczególności zgodnie z ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn.: Dz. U. z 2016 r. poz. 666 z późn. zm.).
7. Sprzęt wchodzący w skład systemów informatycznych musi być objęty odpowiednią ochroną fizyczną. Standardy i szczegółowe procedury bezpieczeństwa fizycznego

opisuje IZSI.

8. Komputery i inne urządzenia przenośne muszą być zabezpieczone w sposób, jaki opisuje IZSI.
9. Osoby upoważnione do przetwarzania danych osobowych, a korzystające z urządzeń przenośnych muszą być świadome zagrożeń i zobowiązane są do zachowania należytej staranności w celu zapewnienia ich bezpieczeństwa zgodnie z postanowieniami IZSI.
10. Zabrania się używania komputerów i urządzeń przenośnych zawierających informacje stanowiące tajemnicę bez zapewnienia ich właściwej ochrony poprzez zastosowanie obowiązujących środków organizacyjno-technicznych i prawnych opisanych w IZSI.

V. Wymiana Danych i Ich Bezpieczeństwo

1. Bezpieczeństwo danych osobowych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach serwera. Pozwala to - przynajmniej w pewnym stopniu - uniknąć wielokrotnego wprowadzania tych samych danych osobowych do systemu informatycznego.
2. Sporządzanie kopii zapasowych następuje w trybie opisanym w IZSI.
3. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach ADO oraz IZSI.
4. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko za zgodą osoby, której dotyczą.
5. Przed atakami z sieci zewnętrznej wszystkie komputery (w tym także przenośne) chronione są środkami dobranymi przez ADO.
6. W zakresie nośników informacji:
   a) wszystkie nośniki informacji podlegają właściwej ochronie stosownie do klasyfikacji informacji, na wszystkich etapach ich używania, od momentu zapisu informacji, aż do momentu wycofania z użycia lub fizycznego zniszczenia opisanego w IZSI;
   b) za zapewnienie właściwej ochrony nośników informacji odpowiada ich użytkownik;
   c) osoby upoważnione do przetwarzania danych osobowych, a korzystające z nośników informacji powinny być świadome zagrożeń, i zobowiązane są do zachowania należytej staranności poprzez zastosowanie obowiązujących środków organizacyjno-technicznych i prawnych opisanych w IZSI;
   d) w przypadku wycofywania z użycia nośników zawierających dane osobowe, na osobie, której nośnik przekazano do używania spoczywa obowiązek wykonania procedury opisanej w IZSI;
   e) urządzenia przenośne oraz nośniki wynoszone z siedziby ADO nie powinny być pozostawiane bez nadzoru w miejscach publicznych;
   f) nie należy pozostawiać bez kontroli dokumentów, nośników i sprzętu w miejscach publicznych ani też w samochodach;
   g) informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu;
   h) w domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do ADO.

VI. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe obejmuje pomieszczenie biurowe zlokalizowane w siedzibie ADO mieszczącej się przy **ul. Bitwy Warszawskiej 1920 r. nr 19.**
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

VII. Postępowanie w Przypadku Naruszenia Ochrony Danych Osobowych

1. Naruszeniem ochrony danych osobowych w rozumieniu Polityki jest każde zdarzenie, zależne jak
   i niezależne od woli ludzkiej, powodujące zagrożenie bezpieczeństwa danych osobowych,
   w szczególności:
   a) prowadzące do utraty integralności danych (np. pozostawianie dokumentów zawierających dane w miejscach powszechnie dostępnych);
   b) zagrażające poufności danych osobowych (np. przesyłanie danych osobowych drogą elektroniczną bez zabezpieczenia dostępu do plików);
   c) zagrażające rozliczalności danych osobowych (np. korzystanie przez kilka osób z jednego hasła dostępu).
2. Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:
   a) stwierdzono naruszenie obowiązujących przepisów wewnętrznych;
   b) stwierdzono naruszenie obowiązujących przepisów prawa;
   c) stwierdzono naruszenie zabezpieczeń fizycznych lub informatycznych;
   d) stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych osobowych;
   e) inne okoliczności wskazujące, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych przez jednostkę.
3. Postanowienia niniejszego rozdziału stosuje się w przypadku naruszenia oraz uzasadnionego podejrzenia naruszenia ochrony danych osobowych.
4. ADO, który stwierdził lub uzyskał informację stwierdzającą albo uzasadniającą podejrzenie naruszenia ochrony danych osobowych, jest zobowiązany niezwłocznie:
   a) wysłuchać relacji zawiadamiającego, jak również każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem, w celu oceny zaistniałej sytuacji;
   b) utrwalić wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności: dokładny czas uzyskania informacji stwierdzającej albo uzasadniającej podejrzenie naruszenia ochrony danych osobowych albo samodzielnego wykrycia tego faktu, dane osoby zgłaszającej, stan zabezpieczeń;
   c) podjąć niezwłocznie wszelkie działania zmierzające do odzyskania utraconych danych osobowych albo zabezpieczenia danych osobowych przed utratą;
   d) podjąć niezwłocznie wszelkie działania zmierzające do ustalenia przyczyn zdarzenia, jak
      i okoliczności sprzyjających naruszeniu;
   e) podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć

przed usunięciem ślady naruszenia ochrony danych osobowych;

f) nawiązać kontakt ze specjalistami spoza firmy, o ile zachodzi taka konieczność.

g) W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych osobowych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż
w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa **Załącznik nr 7**
do niniejszej Polityki.

h) Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane osobowe dotyczą.

5. Do obowiązków ADO w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:

a) osoby upoważnione do przetwarzania danych osobowych były odpowiednio przygotowane
do wykonywania swoich obowiązków,

b) każdy z przetwarzających dane osobowe był pisemnie upoważniony do przetwarzania przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych.

VIII. Powierzenie Przetwarzania Danych Osobowych

1. Administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi (procesorowi) wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO i tylko jeżeli są to dane, które może ujawnić.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.
3. Administrator nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami
w których następuje to na wniosek osoby, której dane osobowe dotyczą.

IX. Postanowienia Końcowe

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2. Każdej osobie upoważnionej do przetwarzania danych ADO udostępnia politykę bezpieczeństwa,
a osobom mającym dostęp do systemów informatycznych dodatkowo również IZSI.
3. Polityka wchodzi w życie z dniem podpisania zarządzenia wprowadzającego.
4. Integralną cześć niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki:

Załącznik nr 1
Wzór rejestru czynności przetwarzania danych osobowych
Załącznik nr 2
Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe
Załącznik nr 3
Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 4
Wzór Oświadczenia i zobowiązania osoby przetwarzającej dane osobowe
Załącznik nr 5
Rejestr osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 6
Instrukcja Zarządzania Systemem Informatycznym - IZIS
Załącznik nr 7
Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego