POLITYKA

BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w

Okręgu Mazowieckim Polskiego Związku Wędkarskiego w Warszawie

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 ze. zm.) oraz § 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024), wprowadza się w Okręgu Mazowieckim Polskiego Związku Wędkarskiego Politykę Bezpieczeństwa Danych Osobowych.

I. Definicje

Użyte w niniejszej Polityce definicje i pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz dla wszystkich pozostałych procedur, instrukcji, dokumentów, które zostały przyjęte przez Okręg Mazowiecki Polskiego Związku Wędkarskiego. Ilekroć jest mowa o:

1. Administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, które decydują o celach i środkach przetwarzania danych osobowych. W niniejszej Polityce przez Administratora danych rozumie się Okręg Mazowiecki Polskiego Związku Wędkarskiego w Warszawie (dalej zwany Administrator lub OMPZW);
2. Administratorze Systemów Informatycznych (zwany dalej ASI) – osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych w zakresie przydzielonych obowiązków z wyłączeniem zadań które zostały przekazane innym podmiotom na podstawie umów powierzenia;
3. Danych osobowych (lub danych) – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4. Dane wrażliwe – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;
5. Dokumentacji przetwarzania danych osobowych – rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych i Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych;
6. Generalnym Inspektorze Ochrony Danych Osobowych (lub GIODO) – rozumie się przez to organ ochrony danych osobowych;
7. Identyfikatorze (loginie) użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8. Osobie fizycznej możliwej do zidentyfikowania – jest to osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nakładu nadmiernych kosztów, czasu lub działań;

9. Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora upoważnienie do przetwarzania danych;
10. Pracownik - osobę zatrudnioną na podstawie stosunku pracy lub umowy cywilno-prawnej;
11. Członek – członek OMPZW;
12. Upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
13. Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych;
14. Rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz.U. Nr 100, poz. 1024);
15. Ustawie – rozumie się przez to ustawę z dnia z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.);
16. Użytkownik – użytkownik systemu informatycznego służącego do przetwarzania Danych osobowych;
17. Załącznikach – należy przez to rozumieć wzory dokumentów; Administrator może przedmiotowe wzory zastąpić wydrukami z systemów komputerowych lub innymi dokumentami o treści zgodnej z przepisami powszechnie obowiązującego prawa;
18. Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

II. Cele i zakres Polityki

1. W celu zapewnienia ochrony przetwarzanych danych osobowych zarówno za pomocą systemów informatycznych jak i w wersji papierowej Administrator wdraża niniejszą Politykę.
2. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane: były przetwarzane zgodnie z prawem, zbierane dla oznaczonych celów, merytorycznie poprawne i adekwatne do celów w jakich są zbierane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą. Wdrożone i stosowane środki techniczne i organizacyjne mają na celu zapewnienie:
   1) poufności – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
   2) integralności – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
   3) dostępności – istnieje możliwość wykorzystania ich na żądanie w założonym czasie przez autoryzowany podmiot,

4) rozliczalności – możliwość jednoznacznego przypisania działań poszczególnym osobom,
5) autentyczności – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
6) niezaprzeczalności – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
7) niezawodności – zamierzone zachowania i skutki są spójne.

3. Administrator deklaruje pełne zaangażowanie i determinację celem zapewnienia bezpieczeństwa przetwarzanych danych osobowych, a także prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych.
4. Administrator na bieżąco dostosowuje systemy informatyczne służące do przetwarzania danych i wszelkie systemy zabezpieczeń przetwarzania danych osobowych do wymogów określonych w rozporządzeniu.
5. Zakres podmiotowy stosowania niniejszej Polityki obejmuje wszystkich pracowników, członków oraz osoby mające dostęp do danych osobowych.
6. Polityka jest dokumentem wewnętrznym, poufnym i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody Administratora.

III. Przetwarzanie danych w OMPZW

1. OMPZW przetwarza dane osobowe w związku z realizacją celów statutowych oraz w ramach bieżącej działalności administracyjnej poprzez:
   1) przetwarzanie danych osobowych członków: w tym przetwarzanie danych zawartych w uchwałach, kwestionariuszach na kandydatów członków Zarządu, Komisji Rewizyjnej, ankietach klubów wędkarskich, rejestrach spraw przewinień członków;
   2) przetwarzanie danych członków i uczestników zawodów sportowych,
   3) przetwarzanie danych osób przystępujących do egzaminów w celu wydania karty wędkarskiej,
   4) sporządzanie list członków w postaci papierowej lub jako zapisy informatyczne dla doraźnych potrzeb np. z tytułu opłacenia składek członkowskich, organizacji zawodów, spotkań, szkoleń, konferencji, darczyńców,
   5) udostępnianie danych innym członkom towarzystwa w celu nawiązania kontaktu, współpracy,
   6) przetwarzanie danych członków w opracowaniach wewnętrznych towarzystwa: sprawozdania, protokoły, raporty,
   7) przetwarzanie danych w publikacjach,
   8) przetwarzanie danych pracowników,
   9) inne wynikające z działalności statutowej.
2. Każdej osobie fizycznej, której dane są przetwarzane w związku z realizacją celów statutowych przysługuje prawo do uzyskania informacji o zakresie jej uprawnień związanych z ochroną danych zgodnie z Ustawą, prawo dostępu do swoich danych osobowych oraz ich poprawiania.

IV. Kompetencje i odpowiedzialność w zarządzaniu ochroną danych osobowych

1. Administrator

1) Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych oraz zabezpiecza posiadane dane przed: ich udostępnieniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem przez osobę nieupoważnioną.
2) Administrator w szczególności zapewnia: przestrzeganie przepisów o ochronie danych osobowych, w szczególności przez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   b) nadzorowanie opracowania i aktualizowania dokumentacji ochrony danych osobowych oraz przestrzegania zasad w niej określonych;
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   d) prowadzenie ewidencji osób upoważnionych;
   e) środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
   f) system i sprzęt informatyczny umożliwiający bezpieczne przetwarzanie danych;
   g) przetwarzanie danych osobowych przez osoby posiadające upoważnienie do przetwarzania danych osobowych;
   h) należyte i terminowe udzielanie informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji w trybie art. 33 ustawy;
   i) kontrolę nad tym jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, usunięte oraz komu i przez kogo przekazane;
3) Do obowiązków Administratora należy zarejestrowanie zbiorów danych osobowych podlegających rejestracji, w rejestrze prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych.

2. Administrator Systemów Informatycznych (ASI)

1) Administrator może wyznaczyć Administratora Systemów Informatycznych.
2) ASI odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych określonych w Instrukcji Zarządzania Systemem Informatycznym.
3) ASI podczas wykonywania obowiązków z zakresu ochrony danych osobowych podlega bezpośrednio Administratorowi.
4) W przypadku niewyznaczenia ASI za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych odpowiada Administrator.

3. Pracownicy, członkowie

1) Wszyscy pracownicy, członkowie są zobowiązani do:
   a) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami niniejszej Polityki i Instrukcji Zarządzania Systemem Informatycznym oraz pozostałymi dokumentami wdrożonych przez Administratora;
   b) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
   c) informowania Administratora o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe;
   d) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia.

2) Pracownicy, członkowie zobowiązani są do stosowania następujących dobrych praktyk. Należą do nich zasady:
   a) polityka czystego biurka w odniesieniu do dokumentów i nośników ruchomych - oznacza, że dokumenty papierowe, listy adresowe, telefoniczne, płyty CD, DVD, pendrivy, telefony komórkowe itp. nie używane w danej chwili i po zakończeniu pracy powinny być przechowywane w bezpiecznym, zamkniętym miejscu;
   b) polityka czystego ekranu w odniesieniu do komputerów i laptopów - oznacza stosowanie wygaszacza ekranu po 15 minutach bezczynności, nie pozostawianie bez nadzoru ww. nośników w stanie zarejestrowania do sieci oraz dbałość o niezamieszczanie na pulpicie ekranu monitora dużej liczny folderów i plików, szczególnie o nazwach wskazujących na ich poufną zawartość;
   c) polityka ochrony urządzeń faksowych, fotokopiarek, innych podobnych pozostających bez nadzoru i niezwłocznego usuwania dokumentów z urządzeń po wydrukowaniu, kopiowaniu;
   d) polityka niszczenia zbędnych dokumentów i zapisów w niszczarkach;
   e) polityka niepozostawiania bez nadzoru i zakazu wynoszenia dokumentów i nośników bez zgody Administratora;
   f) polityka wykorzystywania wyłącznie do celów służbowych dokumentów papierowych, list adresowych i telefonicznych, telefonów komórkowych, sprzętu informatycznego (komputerów, laptopów itp.), nośników informatycznych (przenośnych pamięci, płyt CD, DVD, pendrivów itp.), użytkowanych programów, poczty mailowej i Internetu;
   g) polityka ochrony swojego hasła i zakazu udostępniania haseł do systemów informatycznych.

V. Przetwarzanie danych

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) osoba, której dane dotyczą wyrazi na to zgodę, chyba że chodzi o usunięcie jej danych;
2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

2. Za prawnie uzasadniony cel Administratora uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności oraz marketing bezpośredni własnych produktów lub usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektroniczne należy stosować przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne, które przewidują dalej idącą ochronę.
3. Zgoda na przetwarzanie danych osobowych, nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
4. Zgoda na przetwarzanie danych osobowych może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
5. Zgoda na przetwarzanie danych osobowych może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator obowiązany jest usunąć wszystkie dane osobowe osoby, która zgodę cofnęła, chyba że istnieje inna podstawa prawna upoważniająca Administratora do dalszego przetwarzania tych danych dla innych celów niż wskazany w cofniętej zgodzie.
6. Administrator może powierzyć przetwarzanie danych innemu podmiotowi, w drodze umowy zawartej na piśmie.
7. Podmiot, któremu dane do przetwarzania powierzono, może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.
8. Podmiot, któremu powierzono przetwarzanie danych obowiązany jest przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające przetwarzanie danych, o których mowa w ustawie oraz w rozporządzeniu.

VI. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Administrator prowadzi wykaz zbiorów danych osobowych.
2. Przy opisie każdego ze zbiorów wskazuje się programy zastosowane do przetwarzania danych.
3. Zbiory danych osobowych wraz z programami zastosowanymi do ich przetwarzania stanowią załącznik nr 1 do niniejszej Polityki.

VII. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi. Sposób przepływu danych pomiędzy poszczególnymi systemami

Struktura zbiorów danych osobowych wraz ze wskazaniem poszczególnych pól informacyjnych, powiązania, sposób przepływu pomiędzy nimi wskazane zostały w załączniku nr 2 do niniejszej Polityki.

VIII. Osoby upoważnione do przetwarzania danych osobowych

1. Administrator obowiązany jest nadać upoważnienie do przetwarzania danych każdej osobie przetwarzającej dane.
2. Upoważnienie powinno zwierać:
   1) datę, z którą zostało nadane;
   2) datę, z którą upoważnienie wygasa, jeżeli jest ono nadane na czas określony;
   3) zakres upoważnienia.
3. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy, upływu czasu na jaki zostało nadane.
4. Wzór upoważnienia do przetwarzania danych i oświadczenia o poufności stanowi załącznik nr 3 do niniejszej Polityki.

IX. Ewidencja osób upoważnionych

1. Administrator obowiązany jest do prowadzenia ewidencji osób upoważnionych.
2. Ewidencja może być prowadzona w wersji papierowej lub elektronicznej z możliwością jej wydruku.
3. Ewidencja zawiera:
   a) imię i nazwisko osoby upoważnionej;
   b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
   c) Identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
4. Wzór ewidencji stanowi załącznik nr 4 do niniejszej Polityki.

X. Szkolenia

1. Przed dopuszczeniem osoby upoważnionej do czynności przetwarzania danych Administrator lub upoważniona osoba posiadająca niezbędne kwalifikacje przeprowadza szkolenie z zakresu ochrony danych osobowych.
2. Przeprowadzenie szkolenia może być dokumentowane stosownymi zaświadczeniami lub listą uczestników szkolenia.

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

1. Administrator przetwarza dane w pomieszczeniach do tego przeznaczonych w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.
2. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe zawarty został w załączniku nr 5 niniejszej Polityki.

XII. Określenie środków technicznych, organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych znajduje się w załączniku nr 6 niniejszej Polityki.

XIII. Identyfikacja zagrożeń

Postępowanie w razie zaistnienia zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych lub naruszenia zasad przetwarzania danych osobowych.

Zagrożenia te mogą mieć swoje źródło zarówno w przyczynach, niezależnych od działań ludzkich jak i w działaniach ludzi które mogą być przypadkowe lub umyślne.

Zagrożenia można podzielić na:

Zagrożenia ludzkie	rozmyślne (np.: modyfikacja danych, włamanie do systemu, złośliwy kod, kradzież itp.) W wyniku takiego działania może dojść do zniszczenia danych i zakłócenia ciągłości pracy systemu. Następuje naruszenie poufności i integralności danych.
	przypadkowe (np.: niezamierzone pomyłki i pominięcia, skasowanie pliku - popełnione przez administratorów i operatorów, przerwy w zasilaniu). Działania te mogą prowadzić do utraty integralności danych.
Zagrożenia techniczne	(np.: błędy w działającym oprogramowaniu, wadliwa praca urządzeń sprzętowych, itp.) Może dojść do zakłócenia ciągłości pracy systemu lub utraty danych.

Zagrożenia środowiskowe	(np.: trzęsienie ziemi, powódź, pożar, piorun - wyładowania atmosferyczne) Sytuacje takie powodują zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona. Naruszona zostaje integralność danych i integralność systemu.

Forma przetwarzania danych	Zagrożenie
dane przetwarzane manualnie	– oszustwo, kradzież, sabotaż, – zdarzenia losowe (powódź, pożar), – zaniedbania pracowników (niedyskrecja, udostępnienie danych osobie nieupoważnionej), – niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania, – pokonanie zabezpieczeń fizycznych, – podsłuchy, podglądy, – ataki terrorystyczne, – brak rejestrowania udostępniania danych, – niewłaściwe miejsce i sposób przechowywania dokumentacji,
dane przetwarzane w systemach informatycznych	– nieprzydzielenie użytkownikom systemu informatycznego identyfikatorów, – niewłaściwa administracja systemem, – niewłaściwa konfiguracja systemu, – zniszczenie (sfałszowanie) kont użytkowników, – kradzież danych kont, – pokonanie zabezpieczeń programowych, – zaniedbania pracowników (niedyskrecja, udostępnienie danych osobie nieupoważnionej), – niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania, – zdarzenia losowe (powódź, pożar), – niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych, – naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione, – przypadkowe bądź celowe uszkodzenie, modyfikowanie systemów i aplikacji informatycznych lub sieci, – przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych, – brak rejestrowania zdarzeń tworzenia lub modyfikowania danych.

XIV. Postępowanie w przypadku naruszenia ochrony danych

1. Do przypadków naruszenia zalicza się m.in.:

    1) brak możliwości uruchomienia przez Użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
    2) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
    3) brak możliwości fizycznego dostępu do danych (np. kradzież sprzętu komputerowego, zagubienie klucza do pomieszczeń),
    4) zidentyfikowanie w systemie wirusa lub innego programu, mogącego uszkodzić, skasować bądź skopiować dane osobowe,
    5) stwierdzenie próby bądź podejrzenie nieautoryzowanego przetwarzania danych osobowych (np. zmieniona zawartość zbioru, zmiana kolejności ułożenia dokumentów, otwarte drzwi, nieautoryzowane zniszczenie zawartości zbioru),
    6) naruszenie technicznego stanu urządzeń,
    7) naruszenie zawartości zbioru danych osobowych,
    8) nieskuteczne zniszczenie nośników zawierających dane osobowe (np. nieprawidłowe zniszczenie dokumentu w wersji papierowej, nieprawidłowe usunięcie danych z nośnika np. pendrive),
    9) naruszenie zabezpieczenia systemu informatycznego np. przechwycenie danych przez program szpiegowski,
    10) odtajnienie hasła,
    11) nieautoryzowana zmiana w funkcjonalności aplikacji,
    12) obniżenie jakości/prędkości transmisji danych w sieci telekomunikacyjnej,
    13) niewykonanie kopii zapasowej,
    14) brak możliwości odtworzenia danych z kopii,
    15) powtarzające się zaniki zasilania,
    16) wykorzystywanie przetwarzanych danych osobowych niezgodnie z przepisami ustawy o ochronie danych osobowych,
    17) nieprawidłowości w zakresie zabezpieczenia pomieszczeń gdzie przetwarzane są dane osobowe np. dopuszczenie osoby nieupoważnionej do wglądu w dane osobowe, niewylogowanie się przez użytkownika z systemu w sytuacji opuszczania stanowiska pracy,
    18) wystąpienie sytuacji kryzysowej np. pożar,
    19) użytkowanie stacji roboczej przez osobę nie będącą użytkownikiem systemu,
    20) usuwanie, dodawanie lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
    21) przechowywanie kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

2. Postępowanie w przypadku naruszenia ochrony danych

1) Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych jest zobowiązany do niezwłocznego poinformowania Administratora.
2) W przypadku wykrycia naruszeń w systemie informatycznym służącym do przetwarzania danych lub podejrzenia naruszenia np. pojawienie się wirusa w systemie, poinformowanie Administratora i Administratora Systemów Informatycznych.
3) Po otrzymaniu informacji o wystąpieniu incydentu, który spowodował zagrożenie bezpieczeństwa przetwarzanych danych w systemie informatycznym ASI zobligowany jest do:
   a) Fizycznego odłączenia urządzeń, które umożliwiają nieautoryzowany dostęp do zbioru danych osobowych.
   b) Wylogowania użytkownika, który zgłosił podejrzenie lub naruszenie integralności zbioru danych osobowych.
   c) Podjęcia działań uniemożliwiających dalsze nielegalne przetwarzanie danych osobowych (np. zastosowanie dodatkowych zabezpieczeń, całkowite odłączenie stacji roboczej od zbioru danych osobowych).
   d) Usunięcia skutków incydentu.
   e) Przywrócenie normalnego działania systemu (np. odtworzenie bazy danych z ostatniej kopii).
   f) Zrestartowania hasła użytkownika, który zgłosił naruszenie systemu informatycznego.
   g) Poinformowania o incydencie Administratora, w tym sporządzenia notatki dotyczącej opisu, przyczyn i znanych skutków incydentu.
   h) Wyjaśnienia przyczyn wystąpienia incydentu i podjęcia działań zmierzających do ograniczenia ryzyka wystąpienia ponownego incydentu w przyszłości (np. szkolenie pracowników, analiza wdrożonych środków bezpieczeństwa pod kątem ich skuteczności, ustalenie źródła wirusa i zwiększenie zabezpieczeń).
   i) Wydania decyzji na ponowne rozpoczęcie przetwarzania danych osobowych.
   j) Przedstawienia Administratorowi propozycji poprawy bezpieczeństwa.
4) Administrator przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia. Wzór raportu stanowi załącznik nr 7 do niniejszej Polityki.

XV. Postanowienia końcowe

1) Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie.
2) Wszelkie zmiany dokumentacji przetwarzania danych osobowych obowiązują od dnia ich wprowadzenia w życie.

3) Każdy kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityki.
4) Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
5) W sprawach nieuregulowanych w niniejszej Polityki mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.

Historia zmian

	Wydanie pierwsze	ANNA MARTYNA		
Data	**Zakres zmian**	**Opracował**	**Sprawdził**	**Zatwierdził**