POLITYKA

PRZETWARZANIA DANYCH OSOBOWYCH

W

POLSKIM ZWIĄZKU SZACHOWYM

Załącznik Nr 1 do Uchwały Nr ……
Zarządu Polskiego Związku Szachowego z dnia ……
w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych
w Polskim Związku Szachowym

Na podstawie przepisu art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) wdraża się do stosowania niniejszą Politykę Ochrony Danych Osobowych, zwaną dalej Polityką.

§ 1

POSTANOWIENIA OGÓLNE

1) Polityka została opracowana w celu zapewnienia zgodności procesu przetwarzania danych osobowych z obowiązującymi przepisami prawa, w szczególności z Rozporządzeniem 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), oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000).
2) Celem Polityki jest wskazanie podstaw dla właściwego wykonania obowiązków Administratora danych w zakresie bezpieczeństwa i prawidłowej ochrony przetwarzanych danych osobowych.
3) Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia jako zbiór reguł i zaleceń regulujących sposób ich zarządzania, ochrony i przetwarzania.
4) Polityka zawiera zestaw informacji dotyczących szacowania procesów przetwarzania danych osobowych oraz obowiązujących zabezpieczeń technicznych i organizacyjnych, zapewniających właściwą ochronę przetwarzania danych osobowych.
5) Opracowaną Politykę stosuje się do danych osobowych:
   a) przetwarzanych w systemach informatycznych,
   b) przetwarzanych na nośnikach elektronicznych,
   c) przetwarzanych w sposób tradycyjny.

§ 2

OPISANIE POJĘĆ

Wszystkie pojęcia, definicje oraz skróty zawarte w Polityce są powiązane z innymi dokumentami, które obowiązują w Polskim Związku Szachowym w zakresie ochrony danych osobowych. Określenia użyte w Polityce oraz z w pozostałych dokumentach, o ile nie zaznaczono inaczej, oznaczają:

1) **Administrator danych osobowych (ADO) –** Stowarzyszenie prowadzące działalność pod nazwą Polski Związek Szachowy (dalej w skrócie zwane także PZSzach), która samodzielnie ustala cele i sposoby przetwarzania danych osobowych**;**

2) **Administrator systemu informatycznego (ASI)** – osoba upoważniona przez ADO do zarządzania systemem informatycznym, posiadająca odpowiednią wiedzę z zakresu informatyki;

3) **autentyczność** - właściwość oznaczająca, że zawartość zasobu informacyjnego oraz tożsamość osoby mającej dostęp do tego zasobu, jest taka jak deklarowana;

4) **bezpieczeństwo danych** - stan, w którym informacja jest chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności, zminimalizować straty i zagwarantować zachowanie jej poufności, integralności i dostępności, a dodatkowo również autentyczności, rozliczalności, niezaprzeczalności i niezawodności;

5) **chmura** – miejsce przechowywania danych w systemie informatycznym zlokalizowane poza siedzibą Administratora;

6) **dane osobowe (dane)** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, w rozumieniu przepisów RODO tj. osoby, którą można bezpośrednio lub pośrednio zidentyfikować w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

7) **dostępność danych** – właściwość zapewniająca, że osoby upoważnione mają dostęp do informacji i związanych z nimi zasobów na żądanie i w określonym czasie;

8) **hasło -** ciąg znaków literowych, cyfrowych lub innych znany jedynie użytkownikowi;

9) **identyfikator -** ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

10) **incydent bezpieczeństwa** - każde wykryte naruszenie (albo wykryta próba) naruszenia bezpieczeństwa informacji, będące naruszeniem obowiązujących przepisów wewnętrznych lub przepisów prawa, źródłem incydentu bezpieczeństwa może być zarówno przypadkowe, jak i celowe działanie albo zaniechanie;
11) **integralność danych** – właściwość zapewniająca dokładność i kompletność informacji oraz metod jej przetwarzania;

12) **integralność systemu** – właściwość zapewniająca nienaruszalność systemu i niemożności jakiejkolwiek modyfikacji w sposób nieuprawniony;

13) **Instrukcja zarządzania systemem informatycznym** – instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która została przyjęta i wdrożona w PZSzach, stanowiąca obok Polityki, podstawowy dokument z zakresu ochrony danych osobowych;

14) **naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

15) **niezaprzeczalność danych** – właściwości pozwalająca na ustalenie, że uczestnictwo danej osoby w całości lub części wymiany danych jest niepodważalne, w szczególności poprzez zapewnienie niezaprzeczalności otrzymania danych rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie oraz niezaprzeczalności odbioru danych rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie;

16) **niezawodność danych** – właściwość pozwalająca na ustalenie, że zamierzone zachowania i skutki są spójne;

17) **nośnik danych** – nośnik taki jak papier, płyta, dysk twardy, karta pamięci lub inny, służący do przechowywania i zapisu danych;

18) **personel -** osoby - zatrudnione w Biurze na podstawie stosunku pracy, umów cywilnoprawnych, przedsiębiorcy wykonujący osobiście i jednoosobowo działalność, osoby odbywające staże, praktyki oraz inne osoby wykonujące na zlecenie ADO prace związane z przetwarzaniem danych osobowych;

19) **podmiot przetwarzający** – osoba upoważniona do przetwarzania danych osobowych w imieniu Biura;

20) **poufność danych** - właściwość zapewniająca, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;

21) **przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub każde innego rodzaju udostępnianie, dopasowywanie, łączenie, ograniczanie, usuwanie lub niszczenie;

22) **pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich już było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, przechowywanych osobno i objętych środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

23) **RODO –** Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016r., 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);

24) **ustawa o.d.o. –** Ustawa o ochronie danych osobowych z 10 maja 2018 r. o ochronie danych osobowych Dz.U. z 2018 r., poz. 1000;

25) **ustawa o sporcie –** Ustawa z dn. 25 czerwca 2010 r. o sporcie Dz. U. 2010 Nr 127 poz. 857 z późn. zm.

26) **rozliczalność** - możliwość jednoznacznego przypisania działań danej osoby tylko tej osobie;

27) **system informatyczny** – system współpracujących z sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

28) **udostępnianie danych** – przekazywanie, ujawnianie, rozpowszechnianie danych osobowych odbiorcy danych;

29) **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą;

30) **uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

31) **użytkownik** – członek personelu PZSzach, upoważniony na piśmie do przetwarzania danych osobowych albo inna osoba, która w imieniu lub za zgodą PZSzach upoważniona jest do przetwarzania danych osobowych, której nadano identyfikator lub przyznano hasło dostępu do systemu informatycznego;

32) **zbiór danych** – uporządkowany i posiadający określoną strukturę zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy jest on zcentralizowany czy zdecentralizowany, czy rozproszony funkcjonalnie lub geograficznie;

33) **zgoda** (osoby której dane dotyczą) - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, wyrażone poprzez oświadczenie bądź wyraźne działanie potwierdzające, którym osoba fizyczna, której dane dotyczą, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Skróty użyte w Polityce oznaczają:

1) **CR - Centralny Rejestr PZSzach** – system informatyczny dedykowany do prowadzenia ewidencji klubów – członków PZSzach oraz osób fizycznych – zawodników.

2) **Chessarbiter (w skrócie CA) -** system informatyczny dedykowany do organizacji i przeprowadzania zawodów sportowych, z przeważającą większością zawodów w sporcie szachowym.

3) **Operator systemu CA –** sędzia lub organizator zawodów który uzyskał licencję od właściciela systemu

4) **KEKiR –** Komisja Ewidencji, Klasyfikacji i Rankingu PZSzach

5) **Klub –** organizacja będąca członkiem PZSzach lub kandydatem do członkostwa niezależnie od formy prawnej prowadzonej działalności.
6) **PZSzach** – stowarzyszenie zarejestrowane i działające pod nazwą Polski Związek Szachowy z siedzibą 00-514 Warszawa, ul. Marszałkowska 84/92;
7) **PZS** – Polski Związek Sportowy w rozumieniu Ustawy o sporcie
8) **WZSzach** – Wojewódzki Związek Szachowy w rozumieniu Regulaminu Licencyjnego PZSzach
9) **Zawodnik** - osoba fizyczna która rozpoczęła uprawianie sportu szachowego w grze bezpośredniej w ramach rozgrywek zorganizowanych lub nadzorowanych przez PZSzach na dowolnym poziomie. Obywatele innych krajów mogą być zawodnikami tak samo jak obywatele polscy na podstawie obowiązujących przepisów prawa powszechnego lub przepisów szczególnych PZSzach.

§ 3
ZASADY I PRZESŁANKI ORGANIZACYJNE LEGALIZUJĄCE PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ POLSKI ZWIĄZEK SZACHOWY

Przyjmuje się następujące zasady obowiązujące w PZSzach:

A. Organizacja współzawodnictwa sportowego w sporcie szachowym.

1) Polski Związek Szachowy mający na mocy Ustawy o sporcie status Polskiego Związku Sportowego przetwarza dane osobowe zawodników dla celów:
   a) realizacji, na zasadzie wyłączności, zadania publicznego (zwanego dalej **zadaniem**) określonego w Rozdziale 3 a w szczególności w art. 13 Ustawy o sporcie, polegającego na „realizacji reguł sportowych, organizacyjnych i dyscyplinarnych we współzawodnictwie szachowym” - zgodnie z art. 6 pkt. 1e RODO.
   b) wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy - zgodnie z art. 6 pkt. 1b RODO;
   c) wypełnienia obowiązku prawnego ciążącego na administratorze - zgodnie z art. 6 pkt. 1c RODO;
   d) innych niż wymienione w punktach a, b i c powyżej jeśli osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych - zgodnie z art. 6 pkt. 1a RODO;
2) Dla potrzeb realizacji zadania (określonego w pkt. 1 a powyżej) przyjmuje się następujące zasady:
   a) Dane obowiązkowe zawodnika przetwarzane są w CR dożywotnio.
   b) Dane osobowe zawodników zarejestrowanych dzielą się na:
      i) obowiązkowe publiczne,
      ii) obowiązkowe niejawne,
      iii) inne.
   c) Dane obowiązkowe zawodnika ujawniane publicznie w CR:

(1) Imiona i nazwiska;
(2) Data i miejsce urodzenia;
(3) Unikalny numer systemu informatycznego PZSzach (tzw. ID-CR);
(4) Data rejestracji w CR;
(5) Unikalny numer systemu informatycznego Międzynarodowej Federacji Szachowej (FIDE)
(6) Posiadane kategorie, klasy sportowe, rankingi PZSzach oraz FIDE wraz z historią ich uzyskania.
(7) Informacje o posiadanych licencjach PZSzach oraz datach ich ważności;
(8) Przynależność klubowa zawodnika wraz z historią przynależności;
(9) Informacje o posiadanych odznaczeniach i nagrodach PZSzach;
(10) Informacje o nałożonych karach dyscyplinarnych zgodnie z Regulaminem Dyscyplinarnym PZSzach;
(11) Informację o opłatach należnych do PZSzach i aktualnym stanie ich rozliczenia.
(12) Inne informacje związane z realizacją przepisów prawa z klauzulą jawności

d) Dane obowiązkowe zawodnika podlegające przetwarzaniu niejawnemu w CR:
(1) PESEL
(2) Posiadane orzeczenie o niepełnosprawności;
(3) Poprzednie imiona i nazwiska
(4) Inne informacje związane z realizacją przepisów prawa z klauzulą niejawności

e) CR może obejmować także inne dane zawodnika. Dane te przetwarzane są wyłącznie za zgodą zawodnika i podlegają usunięciu na każde jego żądanie.

f) Zawodnikowi przysługuje prawo do usunięcia danych obowiązkowych (realizacja tzw. prawa do bycia zapomnianym) z Centralnego Rejestru zgodnie z art. 17 pkt. 3 lit. b RODO wyłącznie w przypadku gdy:
- nie posiada kategorii szachowej
- nie został zgłoszony do rejestru FIDE
- nie został ukarany dyscyplinarnie
- usunięcie nie spowoduje ograniczenia praw innego zawodnika

g) Prawo przetwarzania danych nieujawnionych mają wyłącznie upoważnieni administratorzy CR.

3) Zawodników niepełnoletnich reprezentują ich opiekunowie prawni.
4) Uczestnictwo zawodnika w zawodach podlegających ocenie rankingowej (z możliwością wypełnienia norm na kategorię szachową) wymaga rejestracji w CR.
5) Zgłoszenie się zawodnika do zawodów podlegających ocenie rankingowej FIDE skutkuje obowiązkiem przekazania danych osobowych do rejestru FIDE.
6) W celu prowadzenia współzawodnictwa szachowego dane osobowe zawodników zgromadzone w CR, w zakresie ujawnionym publicznie zgodnie z pkt. 2b powyżej, będą udostępniane on-line lub w formie pliku bazy danych licencjonowanym operatorom systemu informatycznego Chessarbiter.
7) Licencjonowani operatorzy systemu Chessarbiter mają każdorazowo obowiązek uzyskać podstawę prawną do przetwarzania danych osobowych każdego zawodnika.

8) W przypadku przeprowadzenia zawodów publicznych podstawę prawną przetwarzania wymaganą w pkt. 7 w sposób wystarczający, w zakresie ujawnionych danych zawodnika, potwierdza rejestracja zawodnika w CR.
9) Publikacja wyników
   a) Publikacja wyników zawodów publicznych w serwisie chessarbiter jest realizowana w zakresie niezbędnym dla zagwarantowania prawa do wolności wypowiedzi i informacji.
   b) Publikacja wyników zawodów niepublicznych dokonywana jest przez licencjonowanych operatorów serwisów na podstawie zgody wszystkich uczestników lub na innej podstawie prawnej. Obowiązek zapewnienia zgodności z prawem spoczywa na operatorze.
10) W przypadku niezastosowania się licencjonowanego operatora systemu do ustaleń pkt. 7 i 8 powyżej PZSzach nie ponosi jakiejkolwiek odpowiedzialności za prawidłowość przetwarzania danych osobowych uczestnika turnieju oraz wynikające z tego konsekwencje.
11) Wyniki wszystkich zawodów opublikowane w systemie informatycznym Chessarbiter traktowane są jak informacja publiczna przez okres minimum 5 lat od dnia zakończenia zawodów. Usuniecie wyników z systemu lub jakakolwiek ingerencja w ich zapisy przed upływem 5 lat możliwa jest wyłącznie:
   a) na żądanie głównego organizatora zawodów,
   b) na podstawie pisemnej zgody wszystkich uczestników zawodów,
   c) na podstawie uchwały Zarządu PZSzach lub prawomocnej decyzji organu dyscyplinarnego PZSzach,
   d) na podstawie przepisu prawa powszechnego lub decyzji uprawnionego organu wydanej na podstawie takiego przepisu.

   Po upływie okresu 5 lat wyniki mogą zostać usunięte na żądanie każdego uczestnika zawodów.
12) Zawodnicy zarejestrowani w CR przed wejściem w życie niniejszej polityki powinni zostać poinformowani o treści tego dokumentu drogą mailową (jeśli są znane adresy) lub poprzez publikację Polityki na stronie internetowej PZSzach.
13) Wypełnione formularze rejestracyjne licencyjne itp. zawodników w formie papierowej podlegają docelowemu zarchiwizowaniu w siedzibie PZSzach.
14) Każdy WZSzach co najmniej raz w roku przekazuje zgromadzoną dokumentację papierową do PZSzach. Dokumentacja musi być uporządkowana w sposób umożliwiający prawidłową archiwizację dokumentów.
15) KEKiR co najmniej raz w roku przekazuje zgromadzoną dokumentację papierową do PZSzach. Dokumentacja musi być uporządkowana w sposób umożliwiający prawidłową archiwizację dokumentów.

B. Pozostała działalność organizacyjna w sporcie szachowym

1) Dane osobowe mogą być przetwarzane w celu organizacji innych niż zawody imprez (jak kursy, zebrania, zgrupowania, wyjazdy reprezentacji itp.).
   a) Protokoły egzaminacyjne w formie papierowej podlegają wieczystej archiwizacji w siedzibie PZSzach.

b) Inne dokumenty zawierające dane osobowe (jak formularze rejestracyjne, listy uczestników, sprawozdania) podlegają zniszczeniu oraz usunięciu z systemów informatycznych niezwłocznie gdy ich przechowywanie stało się niecelowe.

2) Zapisy Polityki nie dotyczą ewidencji zawodników uczestniczących w rozgrywkach szachów korespondencyjnych. Ewidencję zawodników i organizację tych rozgrywek prowadzi Świętokrzyski Związek Szachowy z siedzibą w Kielcach.

C. Pozostała działalność statutowa

1) W zakresie działalności nieopisanej w podrozdziałach A i B powyżej Polski Związek Szachowy działa jako stowarzyszenie w rozumieniu Ustawy Prawo o stowarzyszeniach (Dz.U. 2019 poz. 713) i przetwarza dane osobowe dla celów:
   a) wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy - zgodnie z art. 6 pkt. 1b RODO;
      Punkt ten dotyczy w szczególności wykonania zobowiązań wynikających z: umów o pracę, umów cywilno-prawnych, umów stypendialnych, umów dostarczenia prenumeraty, umów z członkami kadr narodowych, umów sponsorskich itp.
   b) wypełnienia obowiązku prawnego ciążącego na administratorze - zgodnie z art. 6 pkt. 1c RODO;
      Punkt ten dotyczy w szczególności wykonania zobowiązań wynikających z przepisów prawa dotyczących sprawozdawczości, przepisów podatkowych, karno-skarbowych itp.
   c) innych niż wymienione w punktach a, b i c powyżej jeśli osoba której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych - zgodnie z art. 6 pkt. 1a RODO;

§ 4
PRZESŁANKI PRAWNE LEGALIZUJĄCE PRZETWARZANIE DANYCH OSOBOWYCH

1) Dane osobowe w PZSzach są:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty;
   b) zbierane w celach konkretnych, wyraźnie określonych i prawnie uzasadnionych i nie mogą być przetwarzane w sposób niezgodny z tymi celami;
   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
   d) prawidłowe, uaktualniane w razie potrzeby, a także usuwane lub prostowane w razie ustalenia, że są nieprawidłowe w świetle celu ich przetwarzania;
   e) przechowywane w formie ułatwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy niż jest to niezbędne dla celów, w jakich następuje ich przetwarzanie, z zastrzeżeniem wyjątków przewidzianych w RODO;
   f) przetwarzane w sposób zapewniający ich integralność i poufność, a także rozliczalność.
2) Przetwarzanie danych osobowych jest zgodne z prawem, jeśli:
   a) osoba, której dane dotyczą wyraziła na to zgodę;

b) przetwarzanie jest niezbędne do wykonania umowy łączącej PZSzach z osobą, której dane dotyczą, w szczególności do wykonania umów z usługodawcami, członkami personelu lub innymi osobami związanymi z PZSzach stosunkiem prawnym;
c) przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą;
d) przetwarzanie jest niezbędne do wypełnienia ciążącego na PZSzach obowiązku prawnego;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez PZSzach lub przez osobę trzecią, z wyłączeniem sytuacji określonych w RODO;
g) przetwarzanie jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;
h) przetwarzanie jest niezbędne do wykonania powierzonych ADO zadań realizowanych na podstawie umów zawartych z ZUS, NFZ, a także innych umów, jakie w przyszłości mogą zostać zawarte między ADO a podmiotami publicznymi w rozumieniu przepisów powszechnie obowiązującego prawa.

3) Przesłanki legalizujące przetwarzanie danych osobowych mogą wystąpić samodzielnie i niezależnie od siebie, albo jednocześnie i łącznie.
4) PZSzach informuje osobę, której dane dotyczą o podstawie przetwarzania jej danych osobowych, a w przypadkach określonych w ust. 2 pkt h również o podstawie przetwarzania danych osobowych innej osoby fizycznej. Realizacja obowiązku informacyjnego może polegać na umieszczeniu informacji w miejscu ogólnie dostępnym, w siedzibie PZSzach albo na jego stronie internetowej.

§ 5 OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

1) **ADO** zobowiązany jest do podjęcia wszelkich działań, których celem jest zapewnienie prawidłowej ochrony danych osobowych, w szczególności zapewnienie przetwarzania danych ze szczególną starannością realizując następujące zasady:
a) przetwarzanie zgodnie z przepisami prawa,
b) zbieranie danych dla określonych celów i niepoddawanie dalszemu przetwarzaniu niezgodnie z tymi celami,
c) dane będą merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, jednak nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
e) zabezpieczenie środkami technicznymi i organizacyjnymi, które zapewnią rozliczalność, poufność i integralność.
2) W PZSzach stosuje się zabezpieczenie, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia lub też minimalizacja strat związanych ze zrealizowanym zagrożeniem: program antywirusowy, anonimizacja, pseudonominizacja, procedury bezpieczeństwa.

§ 6

AKTUALIZACJA DOKUMENTACJI ZWIĄZANEJ Z OCHONĄ DANYCH OSOBOWYCH

1. Niniejsza Polityka oraz wszystkie dokumenty z nią powiązane powinny być aktualizowane wraz ze zmianami w przepisach prawa dotyczącymi ochrony danych osobowych oraz zmianami wynikającymi z organizacji i funkcjonowania PZSzach.
2. W przypadku potrzeby wynikającej ze zdarzeń związanych z naruszeniem ochrony danych osobowych należy dostosować dokumentację do właściwych procedur, które w sposób skuteczny będą chroniły dane osobowe.
3. W każdym przypadku zmiany zapisów niniejszej Polityki wymagają aktualizacji innych dokumentów powiązanych z Polityką.
4. O wszelkich zmianach w dokumentacji powinni być informowani użytkownicy.

§ 7

ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

1) Celem właściwej realizacji zamierzeń a także skutecznej ochrony danych osobowych należy stosować następujące obowiązki:
   a) przeszkolić pracowników uprawnionych do przetwarzania danych osobowych w zakresie zasad bezpieczeństwa,
   b) przypisać użytkownikom określone cechy pozwalające na ich identyfikację w systemach informatycznych, dające możliwość dostępu do przetwarzania danych osobowych odpowiednio do zakresu upoważnienia,
   c) okresowo kontrolować użytkowników sposób postępowania przy przetwarzaniu danych osobowych,
   d) w przypadku stwierdzonych nieprawidłowości podejmować stosowne działania celem ich wyeliminowania,
   e) na bieżąco wdrażać nowe rozwiązania organizacyjne i techniczne, które wzmocnią bezpieczeństwo przetwarzania danych osobowych.
2) W procesie nadzoru należy szczególnie uwzględniać zabezpieczenie w zakresie integralności, poufności oraz rozliczalności przetwarzania danych osobowych.
3) W procesie zarządzania należy stosować działania które spowodują że pracownicy oraz użytkownicy zewnętrzni będą:
   a) odpowiednio przygotowani i wprowadzeni do przetwarzania danych osobowych,
   b) zapoznani z obowiązującymi w PZSzach procedurami i zasadami przetwarzania danych osobowych
   c) na bieżąco informowani o wszelkich zmianach w procedurach.

§ 8

ODPOWIEDZIALNOŚĆ ADMINISTRATORA DANYCH OSOBOWYCH

1) ADO jest odpowiedzialny za prawidłowe przetwarzanie danych osobowych i ich ochronę zgodnie z obowiązującymi przepisami prawa. Ponadto jest obowiązany do stosowania odpowiednich procedur zapewniających prawidłowe przetwarzanie danych osobowych, a także za zapewnienie ochrony przed zmianą, uszkodzeniem lub zniszczeniem danych osobowych przez nieuprawnioną osobę.
2) Do kompetencji ADO należy:
   a) określenie celów oraz strategii działań w zakresie ochrony danych osobowych,
   b) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
3) Do obowiązków ADO należy:
   a) zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
   b) opracowanie i wdrożenie dokumentacji związanej z ochroną danych osobowych,
   c) nadawanie upoważnień pracownikom oraz użytkownikom zewnętrznym do przetwarzania danych osobowych,
   d) zapewnienie ochrony fizycznej pomieszczeń, w których są przetwarzane dane osobowe,
   e) zapewnienie ochrony danych osobowych przetwarzanych w systemach informatycznych oraz nieinformatycznych,
   f) prowadzenie i aktualizacja rejestru czynności i rejestru kategorii przetwarzania.

§ 9 ODPOWIEDZIALNOŚĆ PRACOWNIKÓW I UZYTKOWNIKÓW SYSTEMU

1) W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest szczególne zaangażowanie ze strony każdego użytkownika w zakresie ochrony danych osobowych.
2) Użytkownicy zobowiązani są do informowania ADO bezpośrednio o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe.
3) Użytkownicy są zobowiązani do:
   a) postępowania zgodnie z Polityką,
   b) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
   c) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.
   d) wykonywania niezbędnych działań w procesie przetwarzania danych celem zapewnienia właściwej ich ochrony. W tym celu powinni:
      i) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
      ii) przestrzegać procedur związanych z dostępem do systemów informatycznych w tym obowiązku regularnych zmian indywidualnych haseł dostępowych oraz ochronę dostępu osób niepowołanych do powierzonych terminali systemów informatycznych
      iii) informować ADO o podejrzanych osobach poruszających się w obszarze przetwarzania danych osobowych,

iv) na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać ADO projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu bezpieczeństwa ochrony danych osobowych.

§ 10

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE ZASAD OCHRONY DANYCH OSOBOWYCH

Rozporządzenie ogólne o ochronie danych osobowych a także Kodeks Karny określają odpowiedzialność pracownika w przypadku naruszenia ochrony danych osobowych.

§ 11

SZKOLENIA

1) Przed rozpoczęciem przetwarzania danych osobowych każdy użytkownik, stażysta, praktykant itp. powinien zostać przeszkolony przez ADO. Szkolenie powinno obejmować następujące zagadnienia:
   a) obowiązujące przepisy w zakresie ochrony danych osobowych,
   b) procedury oraz zasady przetwarzania danych osobowych,
   c) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych,
   d) zasady użytkowania oprogramowania, urządzeń i systemów informatycznych służących do przetwarzania danych osobowych,
   e) rodzaje zagrożeń jakie mogą być związane z przetwarzaniem danych osobowych w systemach informatycznych,
   f) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
   g) zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego,
   h) odpowiedzialność w przypadku naruszenia ochrony danych osobowych,
2) Po przeszkoleniu każda osoba podpisuje oświadczenie o odbytym szkoleniu i zapoznaniu się z przepisami prawa (oświadczenie stanowi załącznik nr 3 do Polityki).
3) ADO prowadzi ewidencję osób przeszkolonych (załącznik nr 1 do Polityki).

§ 11

ZASADY SZCZEGÓLNEJ STARANNOŚCI

Każdy użytkownik dla właściwego sposobu i zasad przetwarzania danych osobowych zobowiązany jest do zachowania szczególnej staranności przy przetwarzaniu danych osobowych, a w szczególności:

1) stosowania wszelkich metod zabezpieczeń wynikających z Polityki,

2) zabezpieczenia wydruków elektronicznych, a także tych, które mogą być tworzone w trakcie kserowania, kopiowania, skanowania
3) udzielania informacji zawierających dane osobowe tylko osobom lub podmiotom uprawnionym,
4) prowadzenie rozmów telefonicznych w sposób bezpieczny tak aby osoba nieuprawniona nie pozyskiwała informacji jeżeli nie jest ona dla niej przeznaczona.

§ 12

MIEJSCA I POMIESZCZENIA PRZEZNACZONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe można przetwarzać wyłącznie w miejscach bezpiecznych i będących pod właściwym nadzorem osoby, która przetwarza i nadzoruje przetwarzanie danych osobowych,
2. Pomieszczenia bezpieczne to takie, które nie są pozostawione bez nadzoru odpowiedzialnego użytkownika,
3. Pomieszczenia w których są przetwarzane dane osobowe są zamykane na klucz podczas nieobecności osoby upoważnionej/nadzorującej.
4. Obiekt, jak i inne pomieszczenia, są zabezpieczone fizycznie zgodnie z obowiązującymi procedurami i potrzebami.
5. W przypadku wykonywania prac naprawczych, remontowych, montażowych przez firmy zewnętrzne, pomieszczenie jest pod stałym nadzorem osoby upoważnionej.
6. Przechowywanie kopii zapasowych powinno być realizowane w innym pomieszczeniu niż znajdują się zasoby podstawowe.
7. Każdy użytkownik w przypadku zauważenia uchybień w zabezpieczeniu pomieszczenia zobowiązany jest niezwłocznie poinformować o tym fakcie ADO.

§ 13

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika upoważnienia do przetwarzania danych osobowych podpisanego przez ADO.
2. Wzór upoważnienia stanowi załącznik nr 2 do Polityki.
3. ADO prowadzi dla pracowników szkolenia z zakresu obowiązujących przepisów prawa i procedur zawartych w Polityce.
4. Pracownik po przeszkoleniu podpisuje oświadczenie o zapoznaniu się z przepisami i procedurami.
5. Wzór oświadczenia stanowi załącznik nr 3 do Polityki.
6. Upoważnienie oraz oświadczenie jest przechowywane w dokumentacji ADO.

§ 14

EWIDENCJA OSÓB UPOWAŻNIONYCH

1. ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
2. Ewidencja jest prowadzona na bieżąco.
3. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Biurze stanowi załącznik nr 1 do Polityki.

§ 15

REJESTR CZYNNOŚCI PRZETWARZANIA

1) ADO prowadzi rejestr czynności przetwarzania danych osobowych, który zawiera:
   a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora;
   b) cele przetwarzania;
   c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   e) informację o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, z podaniem nazwy tego państwa trzeciego lub organizacji międzynarodowej i innych informacji wynikających z RODO;
   f) planowane terminy usunięcia poszczególnych kategorii danych, chyba że nie jest to możliwe do przewidzenia „z góry”;
   g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, zgodnych z RODO.
2) Rejestr prowadzony jest w formie pisemnej lub elektronicznej. Wzór rejestru czynności przetwarzania stanowi załącznik nr 6 do Polityki.

§ 16

REJESTR PRZETWARZANIA DANYCH I REJESTR KATEGORII PRZETWARZANIA

1. Pracownicy powinni w porozumieniu z ADO współpracować w zakresie zgłaszania lub aktualizacji rejestru przetwarzania danych osobowych.
2. ADO prowadzi rejestr czynności przetwarzania danych i rejestr kategorii przetwarzania.

§ 17

UDOSTĘPNIANIE DANYCH OSOBOWYCH – ZASADY, PROCEDURY

1. Udostępnianie danych osobowych odbywa się na zasadzie potrzeby koniecznej,
2. Udostępnianie danych osobowych innym podmiotom odbywa się w oparciu o obowiązujące przepisy lub po uzyskaniu zgody osoby, od której uzyskano dane osobowe.
3. W przypadku udostępniania danych osobowych na zewnątrz ADO dokonuje oceny sposobu przygotowania danych, a także analizuje sposób i prawidłowość przygotowania danych do udostępnienia,
4. Dane osobowe przekazywane na zewnątrz są przekazywane listem poleconym za zwrotnym poświadczeniem odbioru lub innym bezpiecznym sposobem określonym wymogami prawa lub umową,
5. Fakt udostępnienia danych należy udokumentować pisemnie poprzez wykonanie pisma przewodniego lub notatki urzędowej.

§ 18

DOSTĘP, SPROSTOWANIE I USUNIĘCIE DANYCH OSOBOWYCH

1) ADO na wniosek osoby, której dane dotyczą umożliwia jej dostęp do danych oraz udziela informacji w zakresie określonym w ogólnym rozporządzeniu o danych osobowych.
2) ADO na żądanie osoby, której dane dotyczą dokonuje sprostowania danych osobowych lub ich uzupełnienia. Osoba jest zobowiązana do złożenia żądania w formie pisemnej.
3) ADO po złożeniu wniosku przez osobę której dane dotyczą ma obowiązek usunięcia jej danych osobowych w przypadku gdy:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b) osoba której dane dotyczą cofnęła zgodę na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
   c) osoba której dane dotyczą wniosła skuteczny sprzeciw wobec przetwarzania.
   d) dane osobowe były przetwarzane niezgodnie z prawem;
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.

§ 19

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1) Powierzenie danych osobowych odbywa się na zasadach określonych w ustawie o.d.o.
2) Powierzenie danych występuje wówczas, gdy podmiot zewnętrzny ma dostęp do danych osobowych przetwarzanych przez PZSzach.
3) ADO może powierzyć innemu podmiotowi współpracującemu z PZSzach na zasadzie wynikającej z umowy powierzenia. Wzór umowy stanowi załącznik do Polityki.
4) Umowę powierzenia należy zawrzeć na piśmie, umowa powinna zawierać następujące warunki i zawierać:

a) cel i zakres przetwarzania danych osobowych,
b) sposoby zabezpieczenia danych i zasady ich przetwarzania,
c) zasady organizacyjne i techniczne, jakie powinien spełnić podmiot, któremu powierzono przetwarzanie danych osobowych,
d) odpowiedzialność podmiotu, któremu powierzono dane osobowe za nieprawidłowe przetwarzanie danych osobowych,
e) prawo do kontroli podmiotu, któremu powierzono dane osobowe przez przedstawiciela PZSzach.

§ 20

ZASADY POSTĘPOWANIA W PRZYPADKU NARUSZENIA LUB PODEJRZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1) Użytkownicy są zobowiązani do szczególnej staranności przy przetwarzaniu danych osobowych.
2) Użytkownicy każdorazowo przed przystąpieniem do pracy są zobowiązani do dokonania oceny i oględzin miejsca pracy pod kątem, czy nie dokonano jakichkolwiek nieuprawnionych działań związanych z ochroną danych osobowych przez osoby nieuprawnione.
3) Sytuacje, na które należy zwrócić szczególną uwagę to:
   a) próba nieuprawnionego dostępu do pomieszczenia lub dostępu do danych osobowych,
   b) naruszenie lub próba naruszenia integralności, poufności lub rozliczalności danych i systemu,
   c) niezamierzona zmiana lub utrata danych zapisanych na nośnikach jako kopie zapasowe,
   d) próba nieuprawnionego logowania lub inny sygnał wskazujący na próbę lub działanie wskazujące na nielegalny dostęp do systemu,
   e) losowe zdarzenia, takie jak brak zasilania, pożar itp.,
   f) stwierdzenie braku sprzętu informatycznego, jego części lub nośników zewnętrznych zawierających dane osobowe (wydruki, pamięć zewnętrzna, płyty CD, dysk twardy, itp.).
4) W sytuacji, gdy użytkownicy stwierdzą naruszenie lub próby naruszenia ochrony danych osobowych, wówczas są zobowiązani do niezwłocznego poinformowania o tym fakcie ADO.
5) Przed poinformowaniem ADO o naruszeniu lub próbie naruszenia ochrony danych osobowych, użytkownik jest zobowiązany do:
   a) wstrzymania pracy, a także wykonywania jakichkolwiek działań, które mogłyby utrudnić ocenę i analizę stwierdzonych działań związanych z naruszeniem ochrony danych osobowych,
   b) zabezpieczenia materiałów, dokumentów, aby uniemożliwić dostęp osobom nieuprawnionym i dalsza stratę,
   c) wykonywania wskazówek ADO.
6) ADO powinien:
   a) dokonać oceny sytuacji, szczególnie dokonać oględzin stanowiska pracy, pomieszczenia, stanu zabezpieczenia pomieszczenia, potencjalne skutki związane z naruszeniem ochrony danych osobowych,
   b) podjąć dalsze działania stosowne do potrzeb i zaistniałej sytuacji.

7) ADO jest zobowiązany do sporządzenia raportu z naruszenia ochrony danych osobowych (wzór raportu stanowi załącznik nr …… do Polityki).
8) ADO jest zobowiązany w terminie 72 godzin po stwierdzeniu naruszenia, zgłosić takie naruszenie organowi nadzorczemu, chyba że jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
9) Sytuacja związana z naruszeniem lub próbą naruszenia ochrony danych osobowych powinna być przedmiotem analizy i wniosków celem uniemożliwienia podobnych zdarzeń w przyszłości.

§ 21

ZBIORY DANYCH OSOBOWYCH

1. Dane osobowe przetwarzane są w zbiorach z wykorzystaniem systemów informatycznych lub w formie papierowej.
2. Zbiory danych osobowych zamieszczone w systemach informatycznych zlokalizowane są w chmurze lub na nośnikach danych zlokalizowanych w pomieszczeniach biura PZSzach.
3. Zbiory danych osobowych w formie papierowej zlokalizowane są w pomieszczeniach biura PZSzach oraz okresowo w siedzibach WZSzach. WZSzach nie rzadziej niż raz w roku przekazują zarchiwizowane dokumenty do siedziby PZSzach.

§ 22

OCHRONA DANYCH OSOBOWYCH W ZBIORACH NIEINFORMATYCZNYCH

1. Zbiory i dane przetwarzane w tych zbiorach to takie dane, które są przetwarzane w formie tradycyjnej bez wykorzystywania systemów informatycznych.
2. Dane osobowe w formie dokumentów i wydruków podlegają ochronie, a także odpowiedniemu ich zabezpieczeniu w meblach biurowych zamykanych na klucz.
3. Dokumenty, wydruki podlegające zniszczeniu należy zniszczyć skutecznie, tak by osoba nieuprawniona nie mogła zapoznać się z treścią tych dokumentów lub wydruków.
4. W trakcie niszczenia dokumentów należy przestrzegać przepisów prawa.

§ 23

POSTANOWIENIA KOŃCOWE

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy rozporządzenia ogólnego o ochronie danych osobowych i innych ustaw.

ZAŁĄCZNIKI

Załącznik Nr 1	Instrukcja zarządzania systemem informatycznym pod nazwą Centralny Rejestr PZSzach
Załącznik Nr 1.1	Wzór upoważnienia do przetwarzania danych w Centralnym Rejestrze PZSzach (pracownicy etatowi PZSzach – załącznik do umowy o pracę)
Załącznik Nr 1.2	Wzór umowy powierzenia przetwarzania danych w Centralnym Rejestrze PZSzach współpracownikom PZSzach (Administratorzy techniczni, Członkowie Zarządu PZSzach, Członkowie KEKiR, Administratorzy Wojewódzcy CR)
Załącznik Nr 1.3	Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych w Centralnym Rejestrze
Załącznik Nr 2	Instrukcja zarządzania systemem informatycznym pod nazwą Chessarbiter
Załącznik Nr 3	Wzór licencji operatora systemu Chessarbiter.
Załącznik Nr 4	Oświadczenie pracownika/współpracownika o zapoznaniu się z obowiązującymi zasadami ochrony danych osobowych
Załącznik Nr 5	Wzór odwołania upoważnienia.
Załącznik Nr 6	Wzór wypowiedzenia umowy powierzenia.
Załącznik Nr 7	Polityka czystego biurka.
Załącznik Nr 8	Wzór raportu z naruszenia ochrony danych osobowych
Załącznik Nr 9	Spis inwentaryzacyjny baz danych osobowych PZSzach
Załącznik Nr 10	Rejestr przetwarzania danych osobowych.
Załącznik Nr 11	Rejestr kategorii przetwarzania.
Załącznik Nr 12-15	Formularze Ewidencyjne zawodników (załączniki do Regulaminu Ewidencyjnego PZSzach)