UCHWAŁA nr 55/UZ/2024

Zarządu Polskiego Związku Łyżwiarstwa Szybkiego

z dnia 04.06.2024

Działając na podstawie § 29 pkt. 24 Statutu Polskiego Związku Łyżwiarstwa Szybkiego uchwala się, co następuje:

§ 1

Zatwierdza się Politykę Ochrony Danych Osobowych w Polskim Związku Łyżwiarstwa Szybkiego, stanowiącą załącznik do niniejszej uchwały.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

Głosowanie:

- ZA – 6
- PRZECIW – 0
- WSTRZYMUJACYCH – 0

Za Zarząd

PREZES PZŁS

Rafał Tataruch

POLITYKA OCHRONY DANYCH OSOBOWYCH.

ORGANIZACJA SYSTEMU OCHRONY DANYCH OSOBOWYCH

w POLSKIM ZWIĄZKU ŁYŻWIARSTWA SZYBKIEGO Z SIEDZIBĄ W WARSZAWIE

Rozdział I
Postanowienia ogólne, definicje

§ 1

1. Celem Polityki Ochrony Danych Osobowych jest zorganizowanie systemu ochrony danych osobowych w **Polskim Związku Łyżwiarstwa Szybkiego z siedzibą w Warszawie** (dalej: PZŁS) oraz wykazanie zgodności z obowiązującymi przepisami, a także zabezpieczenie praw osób których dane dotyczą, oraz interesów PZŁS, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.
2. Polityka ochrony danych osobowych określa stosowane przez Administratora gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i następowało **w sposób zapewniający ochronę praw i wolności osób fizycznych**.
3. Polityka określa obowiązujące w PZŁS zasady i procedury ochrony danych osobowych, sposoby zapewnienia bezpieczeństwa danych osobowych podczas ich **przetwarzania z wykorzystaniem systemów informatycznych oraz w postaci dokumentacji papierowej**.
4. Polityka obowiązuje **wszystkich członków organów Polskiego Związku Łyżwiarstwa Szybkiego** oraz jej pracowników. Jej zasady stosuje się także do **osób fizycznych i podmiotów świadczących usługi** na rzecz PZŁS na podstawie umów cywilnoprawnych, a także w ramach innych stosunków prawnych i faktycznych, gdy w związku z ich realizacją w jakimkolwiek zakresie przetwarza się dane osobowe w imieniu i na rzecz PZŁS.
5. Określone w polityce środki techniczno-organizacyjne oraz inne zastosowane zabezpieczenia w PZŁS mają zapewnić:
   1) **poufność danych** – rozumianą jako właściwość gwarantującą, że dane nie są udostępniane osobom nieupoważnionym - w obrębie PZŁS oraz na zewnątrz;
   2) **integralność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe, którymi dysponuje PZŁS, nie są zmieniane lub niszczone w sposób nieautoryzowany;
   3) **rozliczalność danych** – rozumianą jako przetwarzanie danych osobowych zgodnie z zasadami określonymi w art. 5 RODO oraz jako właściwość zapewniającą, że operacje dokonywane na danych osobowych konkretnej osoby fizycznej mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) **integralność systemu** – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek nieautoryzowanej modyfikacji;
   5) **odporność systemu**– rozumianą jako tolerancję systemu na zakłócenia funkcjonowania o różnym stopniu i charakterze;
   6) **zdolność do szybkiego przywrócenia dostępności danych osobowych** i dostępu do nich w razie incydentu fizycznego lub technicznego;
   7) **regularne testowanie, mierzenie i ocenianie** skuteczności środków technicznych i organizacyjnych przyjętych w celu zapewnienia bezpieczeństwo przetwarzania danych osobowych w PZŁS.

§ 2
Podstawa prawna

Podstawą do opracowania i wdrożenia polityki są:

a) **RODO** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
b) **ustawa** z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

§ 3
Definicje

1. Ilekroć w polityce używa się pojęć zdefiniowanych w art. 4 RODO, są one rozumiane w sposób tożsamy z wynikającym z definicji zawartych w tym przepisie z zastrzeżeniem ust. 2.
2. Ilekroć w polityce jest mowa o:
   a) **administratorze** – rozumie się przez to **Polski Związek Łyżwiarstwa Szybkiego z siedzibą w Warszawie**, w imieniu którego działa Zarząd,
   b) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
   c) **identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   d) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   e) **integralności systemu** – rozumie się przez to właściwość zapewniającą nienaruszalność systemu, niemożność jakiejkolwiek nieautoryzowanej modyfikacji;
   f) **stacji roboczej** – rozumie się przez to komputer wykorzystywany przez użytkownika systemu informatycznego;
   g) **nośniku danych** – rozumie się przez to nośnik służący do zapisu i przechowywania informacji, w tym w szczególności płyty, dyski twarde, nośniki usb, dokumenty papierowe;
   h) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane podmiotom nieupoważnionym;
   i) **powierzeniu przetwarzania danych osobowych** – rozumie się przez to zlecenie dokonywania operacji przetwarzania danych osobowych podmiotowi przetwarzającemu w imieniu i na rzecz administratora na podstawie umowy lub innego instrumentu prawnego (aktu prawnego) zgodnie z art. 28 RODO;
   j) **osobie upoważnionej** – rozumie się przez to każdą osobę działającą na polecenie i z upoważnienia Administratora oraz dokonującą operacji przetwarzania pod jego kierunkiem, nadzorem i na jego rzecz niezależnie od podstawy prawnej wykonywania tych czynności;
   k) **użytkowniku** – rozumie się przez to osobę upoważnioną, której nadano identyfikator i przyznano hasło w systemie informatycznym;
   l) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby fizycznej lub innego podmiotu;
   m) **urządzeniu mobilnym** – rozumie się przez to komputer przenośny, telefon, tablet, nośnik USB, pamięć przenośną oraz inne nośniki i urządzenia służące do przetwarzania danych osobowych wykorzystywane poza obszarem przetwarzania wyznaczonym przez administratora.

Rozdział II
Rozliczalność przetwarzania danych osobowych

§ 4
Dokumenty służące zapewnieniu rozliczalności

1. Dokonywane u Administratora czynności przetwarzania są rejestrowane w **rejestrze czynności przetwarzania** stanowiącym **załącznik nr 1**, a także w **rejestrze wszystkich kategorii czynności przetwarzania** dokonywanych w imieniu Administratorów innych, niż PZŁS, w przypadku przetwarzania na podstawie umowy powierzenia, stanowiącym **załącznik nr 2.**
2. Administrator określił obszar przetwarzania w **opisie obszaru przetwarzania** stanowiącym **załącznik nr 3.**
3. Administrator dokumentuje naruszenia ochrony danych osobowych, prowadząc **rejestr naruszeń**, zgodnie ze wzorem stanowiącym **załącznik nr 4.**
4. W przypadkach, gdy Administrator **upoważnia do przetwarzania danych osobowych i poleca ich przetwarzanie**, dokumentuje tę czynność zgodnie ze wzorem określonym w **załączniku nr 5** oraz prowadzi **ewidencję upoważnień i poleceń przetwarzania danych osobowych** zgodnie z **załącznikiem nr 6.**
5. **Stosuje się pisemne oświadczenia o zobowiązaniu do zachowania w tajemnicy** danych osobowych oraz sposobów zabezpieczenia, a także przestrzegania zasad przetwarzania danych w PZŁS zgodnie z **załącznikiem nr 7.**

6. Za aktualność i adekwatność informacji zawartych w dokumentach, o których mowa w ust. 1-5 **odpowiada osoba indywidualnie wyznaczona przez Administratora** i dokonuje odpowiednich zmian i aktualizacji w ramach bieżących czynności, niewymagających dokonywania zmiany polityki ani ich osobnej akceptacji przez administratora.

§ 5
Rozliczalność

Rozliczalność przetwarzania administrator zapewnia w szczególności poprzez:

1) **bieżącą analizę** charakteru, zakresu, kontekstu i celów przetwarzania, kategorii przetwarzanych danych, kategorii osób, których dane dotyczą, oraz wszelkich okoliczności dotyczących przetwarzania danych osobowych;
2) **zgodność z prawem przetwarzania danych osobowych,** w szczególności poprzez dokonywaną przez Administratora rzetelną i bieżącą analizę podstaw przetwarzania danych określonych w art. 6 oraz art. 9 RODO zarówno wobec wykonywanych operacji przetwarzania w PZŁS, jak i nowo planowanych;
3) **rzetelne przetwarzanie** danych osobowych przez członków organów PZŁS oraz wszystkie osoby działające w jego imieniu i na jego rzecz, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania dokonywane na każdym etapie przetwarzania, podczas każdej z operacji przetwarzania;
4) **przejrzyste przetwarzanie** na każdym etapie, podczas każdej z operacji przetwarzania z uwzględnieniem realizacji praw osoby, której dane dotyczą, w szczególności poprzez informowanie tej osoby o okolicznościach przetwarzania na zasadach określonych w RODO, w tym stosowania klauzul informacyjnych przy zbieraniu danych oraz informowanie o okolicznościach przetwarzania danych na żądane osoby, której one dotyczą;
5) **uwzględnienie zasady ograniczenia celów** przetwarzania, poprzez zbieranie danych w konkretnych, wyraźnych i prawnie uzasadnionych celach, staranne ich oznaczanie przed rozpoczęciem operacji przetwarzania i niedokonywanie przetwarzania, które byłoby niezgodne z tymi celami, rzetelną analizę celów przetwarzania dokonywaną przez Administratora przed rozpoczęciem przetwarzania;
6) **minimalizację danych** poprzez adekwatne posługiwanie się danymi osobowymi, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane, przy czym ocena adekwatności przetwarzania dokonywana jest na bieżąco przez Zarząd zarówno wobec wykonywanych operacji przetwarzania, jak i nowo planowanych, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania, zasady uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych zgodnie RODO ;
7) **prawidłowość i aktualność danych osobowych,** w tym podejmowanie wszelkich, rozsądnych działań przez Administratora, aby dane nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane, w tym zwłaszcza w przypadku żądania osoby, której one dotyczą;
8) **ograniczenie przechowywania** danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których te dane są przetwarzane, z czym związana jest bieżąca analiza Zarządu co do dopuszczalności przechowywania danych osobowych w poszczególnych zbiorach danych lub w ramach poszczególnych procesów przetwarzania z uwzględnieniem przetwarzania wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z RODO;
9) **realizację praw osób, których dane dotyczą,** w tym niezwłoczne reagowanie na żądania oraz dokumentowanie sposobu realizacji żądań;
10) **integralność i poufność danych,** a więc przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych wskazanych w polityce oraz stosowanych w bieżącej działalności jako adekwatne zabezpieczenie;
11) **uwzględnienie ochrony danych w fazie projektowania oraz domyślnej ochrony danych,** w szczególności przed rozpoczęciem przetwarzania, na najwcześniejszym możliwym etapie planowania nowych operacji przetwarzania, zmiany operacji przetwarzania, zastosowania nowych rozwiązań informatycznych, planowania realizacji zadań, procedur, przedsięwzięć, które wymagają przetwarzania danych osobowych;
12) **odpowiednią organizację przetwarzania danych osobowych,** podział zadań z zakresu ochrony danych osobowych oraz wprowadzenie systemu ewidencjonowanych indywidualnych upoważnień i poleceń

przetwarzania pozwalających na ustalenie zakresu kompetencji **osób przetwarzających dane osobowe** u Administratora, a także oświadczeń o zachowaniu w poufności danych osobowych i sposobów ich zabezpieczenia;

13) **określenie obszaru przetwarzania** z uwzględnieniem administrowania dostępem do pomieszczeń oraz przetwarzania z wykorzystaniem urządzeń mobilnych;
14) **rzetelne ustalanie i dokumentowanie zasad współpracy** przy przetwarzaniu danych osobowych w przypadku współadministrowania oraz powierzenia przetwarzania;
15) **analizę zagrożeń naruszeniami ochrony danych osobowych oraz ryzyka naruszenia praw lub wolności osób fizycznych,** odpowiednie jej dokumentowanie i reagowanie w przypadku zagrożeń;
16) **dokumentowanie naruszeń,** analizę naruszeń, wyciąganie wniosków, zapobieganie naruszeniom;
17) **rzetelne prowadzenie dokumentów,** o których mowa w § 4, oraz wszelkiej innej dokumentacji i procedur z zakresu ochrony danych osobowych.

Rozdział III
Organizacja przetwarzania danych osobowych

§ 6
Środki organizacyjne

Dla zapewnienia poufności, integralności i rozliczalności danych osobowych Administrator wdrożył w szczególności następujące środki organizacyjne:

1) opracowano i **wdrożono Politykę;**
2) **prowadzi się dokumenty,** o których mowa w § 4;
3) do przetwarzania danych osobowych **mają dostęp jedynie osoby zobowiązane do zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, a także osoby posiadające pisemne upoważnienie i polecenie** przetwarzania;
4) wszystkie osoby przetwarzające dane osobowe w imieniu i na rzecz PZŁS, w tym członkowie organów PZŁS lub osoby upoważnione są **zobowiązane zachować w tajemnicy** dane osobowe oraz sposoby ich zabezpieczenia przez czas trwania stosunku prawnego łączącego ich z Administratorem oraz po jego ustaniu;
5) **dokumentuje się przypadki powierzenia** przetwarzania danych osobowych, w szczególności poprzez zawarcie stosowanych umów, a także ustala się czy podmioty współpracujące **zapewniają wystarczające gwarancje** wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą;
6) **dokumentuje się przypadki współadministrowania,** w szczególności poprzez zawarcie stosowanych umów, a także ustala się czy współadministrator **zapewnia wystarczające gwarancje** wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą;
7) przy sporządzaniu umów wprowadza się odpowiednie **klauzule poufności;**
8) **wyznaczono obszar przetwarzania;**
9) **ograniczono używanie urządzeń mobilnych;**
10) **analizuje się zagrożenia, ryzyko naruszeń** praw lub wolności osób fizycznych, dokonuje się audytów i **czynności kontrolnych;**
11) **dokumentuje się naruszenia,** analizuje i podejmuje środki w celu zapobiegania im w przyszłości.

§7
Administrator

1. Wykonując obowiązki administratora, Zarząd PZŁS:
   a) **zapewnia** właściwe **zabezpieczenie systemów informatycznych oraz pomieszczeń,** w których przetwarzane są dane osobowe oraz zapewnia odpowiednią infrastrukturę;
   b) **wydaje polecenia** w zakresie bezpieczeństwa danych osobowych;
   c) **żąda od pracowników a także osób współpracujących** na podstawie umów cywilnoprawnych **wyjaśnień w sytuacjach naruszenia bezpieczeństwa** danych osobowych;

d) odpowiada za spełnienie obowiązku prowadzenia **rejestru czynności przetwarzania** danych osobowych i rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innych administratorów;
e) **realizuje prawa osób**, których dane dotyczą na zasadach określonych w RODO;
f) **dokonuje zgłoszenia naruszeń** ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych oraz zawiadamia o naruszeniu osobę, której dane dotyczą;
g) uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wadze zagrożenia, **wdraża odpowiednie środki techniczne i organizacyjne**, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać, a w razie potrzeby środki te poddaje przeglądom i uaktualniania;

2. W celu ochrony wolności i praw osób fizycznych Administrator stosowanie do swoich możliwości organizacyjnych i technologicznych **wdraża środki**, które są zgodne z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych, **polegające m. in. na minimalizacji przetwarzania danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych**.

§ 8
Osoby upoważnione

1. Osoba upoważniona do przetwarzania danych osobowych, bez względu na podstawę stosunku prawnego łączącego ją z Administratorem jest zobowiązana **przetwarzać dane osobowe zgodnie z przepisami** prawa dotyczącymi ochrony danych osobowych, Polityką oraz procedurami z zakresu ochrony danych osobowych obowiązującymi w PZŁS.
2. **Osoba upoważniona może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie** przez Administratora, w granicach poleconego jej przetwarzania danych osobowych, wyłącznie w celu wykonywania powierzonych jej czynności.
3. **Osoba upoważniona** zapewnia, by przetwarzanie danych osobowych w systemie informatycznym każdorazowo było odpowiednio zabezpieczone, w szczególności zabezpiecza stacje robocze i systemy informatyczne loginami i hasłami.
4. **Osoba upoważniona zobowiązana jest do złożenia pisemnego oświadczenia** o zobowiązaniu do zachowania w tajemnicy danych osobowych oraz sposobów zabezpieczenia, a także przestrzegania zasad przetwarzania danych u Administratora.
5. **Osoba upoważniona zobowiązana jest do:**
   1) **zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczania, odpowiedniego zabezpieczania danych** przed ich udostępnieniem osobom nieuprawnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   2) **pilnego strzeżenia nośników danych,** w tym dokumentów, płyt, pamięci przenośnych i komputerów przenośnych, których nie należy pozostawiać bez kontroli w miejscach, w których narażone są na nieuprawnione pozyskanie przez osoby trzecie;
   3) **odpowiedniego fizycznego zabezpieczania dokumentów i innych nośników** danych osobowych poprzez przechowywanie w zamykanych szafach, zamykanych pomieszczeniach, kontrolę dostępu do pomieszczeń;
   4) **odpowiedniego ustawienia ekranów komputerowych** tak, aby osoby postronne nie mogły oglądać ich zawartości, korzystania z wygaszacza ekranu lub innych rozwiązań zabezpieczających;
   5) **przestrzegania swoich uprawnień w systemie ochrony danych osobowych w PZŁS** oraz w systemie informatycznym, w tym korzystania z własnego identyfikatora i hasła;
   6) prowadzenia **korespondencji mailowej** w sposób odpowiednio ją zabezpieczający;
   7) **niewynoszenia poza obszar przetwarzania** na jakichkolwiek nośnikach zbiorów danych lub ich części, chyba że do takiego działania osoba upoważniona jest uprawniona przez administratora lub jest to nieodłącznie związane z wykonywanymi przez nią obowiązkami, a dane osobowe są należycie zabezpieczone przed zniszczeniem, utratą, ujawieniem osobom trzecim;
   8) **starannego usuwania wszelkich wydruków zawierających dane osobowe,** które nie będą wykorzystywane w pracy, tak by ich ponowne wykorzystanie nie było możliwe; rekomenduje się używanie niszczarki;

9) w przypadku korzystania z drukarek ogólnodostępnych, **niezwłocznego zabierania wydruków** z drukarki;
10) w przypadku korzystania z kserokopiarki, **dopilnowania, aby po zakończeniu kopiowania** nie pozostawały w niej kopiowane dokumenty;
11) **niezwłocznego informowania o naruszeniu** ochrony danych osobowych odpowiednio Zarząd.

Rozdział IV
Powierzenie przetwarzania danych osobowych i współadministrowanie

§ 9
Weryfikacja podmiotu przetwarzającego

Administrator, wybierając podmiot przetwarzający, dokłada należytej staranności, by zapewniał on **wystarczające gwarancje** wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

§ 10
Umowa powierzenia przetwarzania

1. Powierzenie danych osobowych podmiotowi przetwarzającemu następuje na podstawie **pisemnej (w tym elektronicznej) umowy zwanej dalej „umową powierzenia"**, określającej przedmiot i czas trwania przetwarzania, charakter oraz cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora i podmiotu przetwarzającego.
2. Przy zawieraniu umowy powierzenia, administrator zapewnia w szczególności **umowne zobowiązanie podmiotu przetwarzającego do wykonywania obowiązków wynikających z art. 28 ust. 3 RODO.**
3. Administrator zapewnia nadzór nad realizacją umowy powierzenia, podejmując wszelkie czynności zmierzające do zapewnienia zgodnego z prawem przetwarzania danych osobowych oraz adekwatnego ich zabezpieczenia, w tym w przypadku podpowierzenia przetwarzania danych osobowych na zasadach określonych w art. 28 ust. 2 i 4 RODO.

§ 11
Współadministrowanie

1. Jeżeli wymagają tego okoliczności Administrator może podjąć decyzję o wspólnym ustaleniu celów i sposobów przetwarzania danych osobowych z innym Administratorem (współadministrowanie).
2. Uzgodnienia wskazane w ust. 1 jest zawierane w formie pisemnej umowy.
3. Umowa o której mowa w ust. 2, w przejrzysty sposób:
   1) określa odpowiednie zakresy odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności obowiązków informacyjnych oraz innych obowiązków względem osób, których dane dotyczą,
   2) wskazuje jak osoby, których dane dotyczą mogą kontaktować się w celu uzyskania informacji i realizacji przysługujących im praw.
4. Osobę, której dane dotyczą, informuje się o współadministrowaniu przy spełnianiu obowiązku informacyjnego odpowiednio na podstawie art. 13 ust. 1-3 oraz art. 14 ust. 1-4 RODO, a także w sposób pozwalający każdemu zainteresowanemu na łatwe pozyskanie tej informacji, w tym przez publikację na stronie internetowej, w materiałach informacyjnych, przy realizacji praw osób, których dane dotyczą.

Rozdział V
Rejestrowanie operacji przetwarzania danych.

§ 12
Rejestrowanie czynności przetwarzania

1. **Administrator prowadzi rejestr czynności** przetwarzania danych osobowych, który zawiera wszystkie elementy wskazane w art. 30 ust. 1 RODO.
2. W przypadku, gdy PZŁS dokonuje przetwarzania jako podmiot przetwarzający, **rejestr kategorii czynności przetwarzania** zawiera wszystkie elementy wskazane z art. 30 ust 2 RODO.
3. Za aktualizację rejestrów, o których mowa w ust. 1 i 2 odpowiada Zarząd PZŁS.

Rozdział VI
Realizacja praw osób, których dane dotyczą

§ 13
Realizacja żądań osób, których dane dotyczą.

1. **Administrator zapewnia realizację praw osób, których dane dotyczą,** wynikających z rozdziału III RODO, a także innych praw określonych w tym rozporządzeniu wprost lub pośrednio wynikających z jego przepisów.
2. **Za realizację praw, o których mowa w ust. 1, odpowiada Zarząd,** w tym za możliwie najszybsze i wyczerpujące przekazywanie osobie, której dane dotyczą, informacji dotyczących realizacji jej żądania, dokumentowanie tych czynności oraz informowanie o ich przebiegu i sposobie rozstrzygnięcia żądania.
3. Administrator **zapewnia, aby osoby, których dane dotyczą, mogły niezwłocznie w sposób niezakłócony kontaktować się** z nim we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO, w szczególności poprzez zamieszczenie stosownej klauzuli informacyjnej na stronie internetowej PZŁS.
4. **Prawo dostępu do danych oraz inne uprawnienia są realizowane z uwzględnieniem wymogów art. 12 RODO, po uprzedniej weryfikacji tożsamości** osoby występującej z żądaniem. **W razie niemożliwości jednoznacznego ustalenia tożsamości** osoby, która występuje z żądaniem realizacji uprawnienia, w tym weryfikacji, czy w danym przypadku żądający jest osobą, której dane dotyczą, **informuje sią ją o tej okoliczności, rekomendując taki sposób komunikacji, który pozwala zweryfikować tożsamość żądającego.**
5. Przekazując informacje osobie, której dane dotyczą, należy zapewnić, aby obejmowały one wyłącznie informacje dotyczące tej osoby i nie zdradzały informacji o innych.
6. Zarząd podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację dla realizacji obowiązków Administratora wynikających z art. 15-22 i art. 34 RODO.
7. Realizacja każdego z praw osoby, której dane dotyczą, następować ma **rzetelnie, niezwłocznie, w terminie nie dłuższym niż miesiąc od otrzymania żądania,** jeśli okoliczności konkretnej sprawy i skomplikowany charakter żądania wymagają dłuższego czasu realizacji, wówczas termin ten można przedłużyć o kolejne dwa miesiące. W terminie miesiąca od otrzymania żądania Zarząd informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
8. Zbierając informacje bezpośrednio od osoby, której dane dotyczą, należy jednocześnie przekazać tej osobie informacje wskazane w art. 13 ust. 1 i 2 RODO. **Obowiązek ten należy zrealizować w trakcie pozyskiwania informacji, dostosowując jego treść do podstaw prawnych przetwarzania,** dotyczy to w szczególności zbierania danych osobowych przy wypełnianiu deklaracji członkowskich przystąpienia do PZŁS.
9. Gdy dane są zbierane z innego źródła niż od osoby, której dotyczą, należy przekazać tej osobie informacje wskazane art. 14 ust. 1 i 2 RODO:
   1) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
   2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
   3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.
10. Stosowną informację w zakresie określonym w art. 13 ust. 1 i 2 lub art. 14 ust.1 i 2 RODO należy podmiotowi danych **przekazać także w przypadku zmiany celu przetwarzania dokonanym po zebraniu danych, chyba że został już o tym uprzedzony.**

§ 14
Zgoda na przetwarzanie danych osobowych

1. Jeżeli zgodnie z art. 6 ust.1 lub art. 9 ust. 2 RODO podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, to **oświadczenie wyrażeniu zgody na przetwarzanie danych powinno być**

dobrowolne, konkretne, świadome i jednoznaczne. Zgoda musi spełniać kryteria rozliczalności i transparentności, w tym wszystkie wymogi określone w art. 7 RODO, a kiedy to uzasadnione okolicznościami, także wymogi określone w art. 8 RODO.

2. **Zapewnia się prawo do wycofania zgody i informuje się o nim** przed złożeniem oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych.

§ 15
Udostępnianie danych osobowych

1. **Administrator decyduje o udostępnieniu danych osobowych** rozumianym jako ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, zapewniając, aby udostępnienie było zgodne prawem.
2. W trybie wnioskowym dane osobowe **udostępniane są tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.**
3. Udostepnienie danych osobowych **musi mieć podstawę odpowiednio w treści art. 6 ust. 1 lub – w przypadku szczególnych kategorii danych – w treści art. 9 ust. 2 RODO.**
4. Dane osobowe mogą być udostępniane **w następujących przypadkach,** jeśli jest to zgodne z przepisami, o których mowa w ust. 3:
   1) z inicjatywy Administratora;
   2) na podstawie wniosku organu władzy publicznej lub innego podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów prawa;
   3) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
5. W miarę możliwości, o ile to uzasadnione okolicznościami, przy udostępnianiu danych osobowych zaznacza się, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
6. O ile jest tu uzasadnione okolicznościami, udostępnienie danych powinno być **udokumentowane w sposób zapewniający rozliczalność przetwarzania,** a także realizację informacyjnych uprawnień osób, których dane dotyczą, w tym wynikających z art. 15 RODO.

Rozdział VII
Zagrożenia i ocena ryzyka

§ 16
Zagrożenia

Administrator podejmuje wszelkie możliwe działania służące zapobieganiu zagrożeniom naruszeniami ochrony danych osobowych, takim, jak w szczególności:

1) **działanie siły wyższej** lub sytuacje losowe, w tym nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne;
2) **niewłaściwe parametry środowiska,** zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);
3) **niewłaściwe posługiwanie się** sprzętem lub oprogramowaniem;
4) **awarie sprzętu lub oprogramowania,**
5) **nieprawidłowe działanie procedur serwisowych,** w tym związane z naprawą sprzętu zawierającego dane osobowe poza obszarem przetwarzania administratora;
6) **rozproszenie danych w Internecie** z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora;
7) **ataki** dokonywane przez Internet oraz poprzez przełamanie zabezpieczeń fizycznych;
8) **naruszenia zasad** określonych w przepisach prawa lub dokumentacji z zakresu ochrony danych osobowych, w tym zwłaszcza:
9) naruszenie bezpieczeństwa danych przez ich **nieautoryzowane przetwarzanie** lub zgoda na takie działania przez inne osoby (np. udostępnienie identyfikatora i hasła innemu użytkownikowi);
10) **ujawnienie** danych osobowych **osobom nieuprawnionym;**

11) **niedostateczny nadzór pomieszczeń**, w których przetwarzane są dane osobowe lub niedostateczny nadzór używanego sprzętu;
12) **niewykonywanie kopii** zapasowych;
13) **brak zabezpieczenia lub niestaranne zabezpieczenie dokumentów** przed zabraniem przez osobę nieuprawnioną, zmianą, uszkodzeniem, lub zniszczeniem, niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska;
14) **przetwarzanie danych osobowych niezgodnie z celem przetwarzania**, w tym w szczególności w celach prywatnych;
15) **samodzielne instalowanie programów bez zgody Administratora;**
16) **niezabezpieczenie** danych osobowych lub systemu informatycznego służącego do ich przetwarzania przed opuszczeniem miejsca pracy lub zakończeniem pracy w systemie informatycznym lub z wykorzystaniem dokumentów;
17) **nieskuteczna anonimizacja** danych osobowych lub nieprawidłowa pseudonimizacja;
18) **nieprawidłowe lub niezgodne z prawem powierzenie** przetwarzania danych;
19) **przetwarzanie nieadekwatne** w stosunku do celu.

§ 17
Ryzyko naruszenia praw lub wolności osoby fizycznej

1. Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych **mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych,** którym **Administrator stara się przeciwdziałać,** wprowadzając politykę oraz podejmując przewidziane w niej środki techniczne i organizacyjne, a także inne środki adekwatne do potrzeb, charakteru, zakresu i kontekstu przetwarzania.
2. **Administrator oraz osoby upoważnione przeciwdziałają wystąpieniu związanych z przetwarzaniem naruszeń praw lub wolności** osoby fizycznej, które mogłyby poskutkować:
   1) dyskryminacją,
   2) kradzieżą tożsamości lub oszustwem dotyczącym tożsamości,
   3) stratą finansową,
   4) naruszeniem dobrego imienia,
   5) naruszeniem poufności danych osobowych chronionych tajemnicą zawodową,
   6) nieuprawnionym odwróceniem pseudonimizacji lub
   7) wszelką inną znaczną szkodą gospodarczą lub społeczną;
3. **Administrator oraz osoby upoważnione przeciwdziałają zagrożeniom** powodującym naruszenie praw lub wolności skutkującym:
   1) pozbawieniem osób fizycznych przysługujących im praw i wolności;
   2) możliwości sprawowania przez osoby fizyczne kontroli nad swoimi danymi osobowymi;
   3) bezprawnemu przetwarzaniu danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych, danych genetycznych, dane dotyczących zdrowia lub seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa;
4. **Administrator oraz osoby upoważnione przeciwdziałają ocenianiu czynników osobowych,** w szczególności analizowania lub prognozowane aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się - w celu tworzenia lub wykorzystywania profili osobistych, chyba, że działania tego rodzaju pozostawałyby w zgodzie z przepisami prawa.
5. **Administrator oraz osoby upoważnione szczególną staranność zachowują przy przetwarzaniu danych osobowych osób wymagających szczególnej opieki,** w szczególności dzieci lub gdy przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

§ 18
Ocena ryzyka i ocena skutków przetwarzania dla ochrony danych

1. **Celem oceny ryzyka jest ustalenie czy stopień bezpieczeństwa danych jest odpowiedni oraz czy nie zachodzi niebezpieczeństwo naruszenia praw lub wolności osób fizycznych.**

2. Administrator **przeprowadza ocenę ryzyka gdy:**
   1) są planowane lub podejmowane nowe operacje przetwarzania danych osobowych;
   2) są planowane lub podejmowane nowe zadania wymagają przetwarzania danych osobowych;
   3) dokonywane są zmiany sposobu działania Administratora w szczególności zmiany w zakresie wykorzystywanej technologii i organizacji pracy, gdy może to mieć wpływ na przetwarzanie danych osobowych.
3. **Wyniki oceny ryzyka są dokumentowane.**
4. Jeśli Administrator zdecyduje się podjąć planowane działania, mimo, że z oceny ryzyka wynika, że z dużym prawdopodobieństwem mogą one powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych:
   1) **stosuje odpowiednie środki zaradcze,** w tym wdraża odpowiednie zabezpieczenia techniczne i organizacyjne,
   2) **powoduje przeprowadzenie oceny skutków ochrony danych osobowych**, o której mowa w art. 35 RODO.
5. Ocenę ryzyka przeprowadza się także w przypadku **stwierdzenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych.**
6. Jeśli ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby nadal wysokie ryzyko naruszenia wolności lub praw osób, których dane dotyczą, a zastosowane środki nie pozwalają na jego zminimalizowanie, administrator rezygnuje z podejmowania planowanych działań albo dokonuje **uprzednich konsultacji z Prezesem Urzędu Ochrony Danych Osobowych zgodnie z art. 36 RODO.**

Rozdział VIII
Środki ochrony danych osobowych i zabezpieczenia

§ 19
Środki zapewnienia ochrony danych osobowych

1. Ochronę przetwarzania danych osobowych zapewnia się przez **wprowadzenie adekwatnych zabezpieczeń, podnoszenie świadomości osób upoważnionych** co do obowiązków wynikających z przepisów prawa o ochronie danych osobowych oraz procedur obowiązujących u administratora.
2. Obowiązki, o których mowa w ust. 1, realizuje **Zarząd**

§ 20
Środki ochrony fizycznej

W celu zapewnienia ochrony przetwarzanych danych osobowych **Zarząd zapewnia zastosowanie następujących środków ochrony fizycznej:**

1) **zamykane** pomieszczenia i kontrolowany dostęp do tych pomieszczeń lub części pomieszczeń, w których przetwarza się dane osobowe;
2) **miejsca przeznaczone do przechowywania dokumentów papierowych odpowiednio zabezpieczone poprzez zastosowanie zamykanych na klucz szaf lub szafek** z możliwością dostępu do nich wyłącznie dla osób upoważnionych do przetwarzania danych osobowych.

§ 21
Polityka kluczy

1. Kluczami do pomieszczeń, w których przetwarza się dane osobowe w formie dokumentacji papierowej lub z wykorzystaniem systemu informatycznego, dysponuje się w sposób określony przez **Zarząd.**
2. Przed rozpoczęciem pracy z wykorzystaniem dokumentów papierowych lub systemów informatycznych drzwi do lokalu otwierają wyznaczone osoby, które są uprawnione do dysponowania kluczami, według tej samem procedury zamyka się drzwi po zakończeniu pracy. Zasadę tę stosuje się analogicznie w przypadku dostępu do szaf, szafek lub innych miejsc, w których przechowuje się dokumenty lub inne nośniki danych osobowych.

Rozdział IX
Zasady dostępu do systemów informatycznych

§ 22
Dostęp do systemów informatycznych

1. O sposobie realizacji dostępu do systemów informatycznych decyduje **Zarząd.**
2. Urządzenia zasilane energią elektryczną, służące w systemach informatycznych do przetwarzania danych osobowych, powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej.
3. Kontroluje się dostęp do pomieszczeń, w których zlokalizowane są stacje robocze, serwerownie oraz węzły sieci teleinformatycznej.

§ 23
Zasady korzystania z systemów informatycznych

1. O przyznaniu użytkownikowi dostępu i udzieleniu uprawnień do zasobów systemu decyduje **Zarząd.**
2. Użytkownikowi nadaje się wyłącznie te uprawnienia w systemie informatycznym, które są konieczne do realizacji przez niego zakresu obowiązków (zasada minimalnych uprawnień).
3. Użytkownik może korzystać tylko z tych zasobów systemów, które są ogólnie dostępne lub do których ma dostęp wyłącznie w dozwolonym dla niego zakresie.
4. Użytkownikowi nie wolno wykorzystywać uprawnień (konta) innego użytkownika, z wyjątkiem sytuacji szczególnych za zgodą Administratora.

Rozdział X
Procedury nadawania uprawnień do przetwarzania danych osobowych w systemie informatycznym oraz uwierzytelnianie

§ 24
Rejestracja użytkownika

1. Uprawnienia użytkownika w systemach informatycznych nadaje się osobom wskazanym przez **Zarząd.**
2. Użytkownikowi **nadaje się identyfikator. Identyfikator użytkownika wykorzystany już w systemie informatycznym nie może być przydzielony innej osobie.**
3. W celu uzyskania dostępu do usług w systemie informatycznym użytkownik jest zobowiązany posługiwać się wyłącznie przydzielonym mu identyfikatorem.

§ 25
Uwierzytelnianie

Uwierzytelnienie użytkownika w systemach informatycznych **następuje za pomocą identyfikatora nadanego użytkownikowi oraz hasła.**

§ 26
Wyrejestrowanie użytkownika

1. Wyrejestrowanie użytkownika z systemu informatycznego polega na odebraniu wszystkich posiadanych uprawnień oraz likwidacji konta użytkownika.
2. Wyrejestrowanie użytkownika następuje z chwilą ustania uprawień do przetwarzania danych osobowych w zakresie wynikającym z przydzielonych zadań niezależnie od ich podstawy pranej. O wyrejestrowaniu użytkownika może zdecydować Zarząd.

§ 27
Hasła

1. Użytkownik systemu ma obowiązek używania hasła zabezpieczającego jego konto.
2. **Hasło:**
   1) **nie może być takie samo jak identyfikator;**
   2) **nie może być tożsame z imieniem, nazwiskiem, datą urodzenia, numerem telefonu, numerem PESEL, ani inną informacją dotyczącą użytkownika lub członków jego rodziny;**
   3) **nie może być krótsze niż 8 znaków;**

4) musi zawierać co najmniej wielkie i małe litery, cyfry i znaki specjalne;
3. Hasła muszą być zmieniane nie rzadziej niż co 6 miesięcy.
4. W miarę możliwości technicznych zapewnia się wymuszanie zmiany haseł przez system informatyczny. Jeśli zmiana hasła nie jest wymuszana, obowiązek przestrzegania częstotliwości zmiany hasła spoczywa na użytkowniku.
5. Hasło należy utrzymać w tajemnicy, również po upływie jego ważności oraz po upływie okresu zatrudnienia. Użytkownik jest odpowiedzialny za zachowanie hasła w tajemnicy. Umożliwienie zapoznania się z hasłem przez inną osobę może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

Rozdział XI
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 28
Rozpoczęcie pracy

Użytkownik zobowiązany jest przestrzegać następujących zasad rozpoczęcia pracy w systemie informatycznym:
1) **należy sprawdzić stan zabezpieczeń pomieszczeń** przy ich otwieraniu, a w razie stwierdzenia ich naruszenia lub śladów obecności w nich osób nieuprawnionych, niezwłocznie zawiadomić Zarząd;
2) **podczas uruchamiania stacji roboczej** należy obserwować ekran monitora, czy nie pojawiają się nietypowe komunikaty mogące świadczyć o nieuprawnionym dostępie do komputera, a w razie stwierdzenia nieprawidłowości poinformować administratora;
3) należy podać swój identyfikator oraz związane z nim hasło w celu uwierzytelnienia się w systemie informatycznym.

§ 29
Zakończenie pracy

Użytkownik zobowiązany jest przestrzegać następujących zasad zakończenia pracy w systemach informatycznych:
1) przed ostatecznym zakończeniem pracy w systemie informatycznym **należy zakończyć wszystkie używane aplikacje** zgodnie z instrukcją obsługi programów;
2) **należy wyłączyć stację roboczą** zgodnie z instrukcją jej obsługi;
3) przed opuszczeniem pomieszczenia **należy upewnić się, czy pomieszczenie to oraz znajdujące się w nim nośniki danych są odpowiednio zabezpieczone,** w tym w szczególności, czy zamknięte są okna, czy nośniki, w tym USB, dyski przenośne, wydruki danych są zabezpieczone w miejscu do tego przeznaczonym i chronione przed szkodliwym oddziaływaniem lub dostępem osób nieuprawnionych oraz czy nie występują zagrożenia mogące mieć wpływ na bezpieczeństwo danych osobowych.

§ 30
Zawieszenie pracy

Użytkownik zobowiązany jest przestrzegać następujących zasad zawieszenia pracy w systemach informatycznych:
1) **należycie zabezpieczyć dostęp do stacji roboczej** podczas zawieszenia pracy w systemie informatycznym lub w czasie tymczasowego opuszczenia stanowiska pracy;
2) w celu ochrony dostępu do komputera podczas zawieszenia pracy w systemie informatycznym, **należy uruchomić wygaszacz ekranu – najlepiej z opcją ochrony hasłem.**

Rozdział XII
Kopie zapasowe i nośniki informacji zawierające dane osobowe

§ 31
Kopie zapasowe

1. W celu zagwarantowania bezpieczeństwa danych przechowywanych w systemach **wykonywane są ich kopie zapasowe, tj. kopie bezpieczeństwa oraz archiwalne.**

2. Bazy danych, oprogramowanie oraz konfiguracja systemów są zabezpieczone w postaci **kopii bezpieczeństwa.**

Rozdział XIII
Sposób zabezpieczenia systemów informatycznych przed działalnością szkodliwego oprogramowania

§ 32
Oprogramowanie

1. **Oprogramowanie stosowane przez Administratora może pochodzić wyłącznie z legalnych źródeł** oraz musi posiadać łatwo dostępną informację o identyfikatorze, wersji i numerze licencji.
2. Wdrożenie modyfikacji istniejącego lub stworzenie albo zakup nowego oprogramowania przetwarzającego dane osobowe możliwe jest wyłącznie w przypadku spełnienia przez oprogramowanie **wymogów z zakresu bezpieczeństwa wynikających z obowiązujących przepisów prawa dotyczących ochrony danych osobowych.**

§ 33
Zabezpieczenie przed szkodliwym oprogramowaniem

1. W celu ochrony systemów przed szkodliwym oprogramowaniem, oprogramowanie antywirusowe podlegające systematycznej aktualizacji **musi być zainstalowane na każdym stanowisku komputerowym.**
2. Każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego.
3. **Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym.**
4. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
5. **W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien:**
   1) odłączyć stanowisko komputerowe od sieci,
   2) zawiadomić o zaistniałym zdarzeniu Zarząd.

Rozdział XIV
Naruszenie ochrony danych osobowych

§ 34
Postępowanie w przypadku stwierdzenia lub podejrzenia stwierdzenia naruszenia ochrony danych osobowych

1. **W przypadku stwierdzenia lub podejrzenia stwierdzenia naruszenia ochrony danych osobowych,** osoba działająca w imieniu i na rzecz PZŁS, członek personelu podmiotu przetwarzającego, współadministratora albo inna osoba ma obowiązek niezwłocznie powiadomić o tym odpowiednio **Zarząd,** a następnie stosować się do podjętych przez niego decyzji i wydanych poleceń.
2. **Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:**
   1) opis przejawów naruszenia ochrony danych osobowych,
   2) opisanie stanu faktycznego i wskazanie miejsca i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych,
   3) wskazanie wszelkich istotnych informacji mogących wskazywać na przyczynę i skutki naruszenia,
   4) wskazanie wszelkich czynności dokonanych po ujawnieniu naruszenia mających wpływ na jego rozmiar lub zmitygowanie.
3. **Zarząd** lub wskazana przez niego osoba przeprowadza niezwłocznie postępowanie wyjaśniające w celu ustalenia czy naruszenie ochrony danych osobowych nastąpiło oraz jakie były jego przyczyny, a w szczególności może:
   1) żądać wyjaśnień od pracowników oraz innych osób upoważnionych, a także członków personelu podmiotu przetwarzającego;
   2) wprowadzić niezbędne środki zaradcze;
   3) nakazać wstrzymanie przetwarzania danych lub ograniczenie w takim zakresie, w jakim jest to niezbędne dla zapobieżenia skutkom naruszenia ochrony danych osobowych lub ustalenia jego przyczyny.

4. Czynności podejmowane w związku z naruszeniem ochrony danych osobowych są dokumentowane .
5. **Zarząd podejmuje decyzję o dalszym trybie postępowania,** a w szczególności:
   1) jeśli to uzasadnione, zarządza podjęcie czynności zmierzających do usunięcia naruszenia i jego skutków oraz zapobieżeniu naruszeniom ochrony danych osobowych na przyszłość,
   2) jeśli to możliwe, zarządza zastosowanie środków eliminujących lub zmniejszających prawdopodobieństwo ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   3) jeśli jest to uzasadnione, zawiadamia o naruszeniu właściwe organy, w tym zgłasza naruszenie organowi nadzorczemu oraz zawiadamia o naruszeniu osoby, których dane dotyczy, odpowiednio zgodnie z art. 33 oraz art. 34 RODO.

§ 35

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu i zawiadomienie osoby, której dane dotyczą.

Jeśli **Zarząd ustali, iż zaistniało prawdopodobieństwo, że stwierdzone naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia** wolności lub praw osób fizycznych, zgłasza naruszenia organowi nadzorczemu zgodnie z art. 33 RODO.

§ 36

Zawiadomienie osoby, której dane dotyczą.

1. Jeżeli **Zarząd ustali, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko** naruszenia wolności lub praw osób fizycznych i nie da się zastosować środków eliminujących to wysokie ryzyko, zawiadamia o naruszeniu dla wszystkie osoby, których danych naruszenie dotyczy.
2. Zawiadomienie, o którym mowa w ust. 1 dokonywane jest na zasadach określonych w art. 34 RODO.

§ 37

Dokumentacja naruszenia ochrony danych osobowych

Dokumentacja naruszeń prowadzona przez **Zarząd** obejmuje w szczególności:
1) **zgłoszenie naruszenia Zarządowi** i udokumentowane ustalenia dotyczące naruszenia,
2) **treść zgłoszenia dokonanego organowi nadzorczemu,** o ile takie zgłoszenie miało miejsce;
3) **treść zawiadomienia, osoby, której dane dotyczą,** o ile takie zawiadomienia miało miejsce;
4) **informację** odpowiednio o przyczynie niezgłaszania naruszenia organowi nadzorczemu lub odstąpienia od zawiadomienie osoby fizycznej, której dane dotyczą;
5) **wszelkie inne dokumenty,** w tym notatki służbowe, pliki, zdjęcia i inne dowody zebrane w trakcie przeprowadzania czynności wyjaśniających pozwalające ustalić okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania nadzorcze;
6) **rejestr naruszeń.**

Rozdział XV
Postanowienia końcowe

§ 38

Zmiany i aktualizacja

1. W związku z dynamiką zmian w zakresie bezpieczeństwa informacji oraz mając na uwadze częste zmiany w konstrukcji systemów informatycznych, Administrator dokonuje przeglądów polityki adekwatnie do tego rodzaju zmian.
2. Polityka podlega aktualizacji każdorazowo w przypadku w przypadku zmiany przepisów prawa dotyczących ochrony danych osobowych mających wpływ na treść i sposób realizacji przewidzianych w niej obowiązków lub procedur.

§ 39

Wejście w życie

Polityka wchodzi w życie z dniem 04 czerwca 2024 roku.