POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W OPOLSKIM ZWIĄZKU TENISA STOŁOWEGO

Z SIEDZIBĄ W OPOLU

Strzelce Op. czerwiec 2018 r.

Spis treści

§ 1. PRZEPISY OGÓLNE

1. Polityka Bezpieczeństwa Danych Osobowych (dalej: **Polityka**) ma za zadanie określać środki techniczne i organizacyjne obowiązujące w:

   Opolskim Związku Tenisa Stołowego z siedzibą przy ul. Damrota 6, 45-064 Opole, wpisanym do rejestru stowarzyszeń Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Opola-Ozimskiej w Opolu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000227352, NIP: 754-26-49-568, REGON: 531624100 (dalej: **Związek**),

   które uznać należy za niezbędne dla zgodności z prawem, rzetelności i przejrzystości, prawidłowości, integralności i poufności oraz rozliczalności przetwarzania danych osobowych w obliczu zagrożeń, przed którymi dane osobowe muszą być chronione. Ponadto, Polityka określa podstawowe zasady zagwarantowania realizacji praw osób, których dane są przetwarzane przez Związek, a w szczególności prawo do ochrony danych.

2. Polityka pozostaje w zgodzie z postanowieniami innych dokumentów obowiązujących w Związku, istotnych w zakresie ochrony danych osobowych.

3. Polityka została opracowana w celu zapewnienia standardów bezpieczeństwa danych osobowych w Związku ze szczególnym uwzględnieniem ich zgodności z przepisami prawa.

4. Postanowienia Polityki pozostają w zgodzie z postanowieniami zawartymi w:
   1) Konstytucji Rzeczpospolitej Polski z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483), ze szczególnym uwzględnieniem postanowień artykułów 47 i 51,
   2) Rozporządzeniu 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 (dalej: **Rozporządzenie Ogólne**),
   3) Ustawie z dnia 26.05.2018 roku o ochronie danych osobowych,
   4) innych powszechnie obowiązujących aktach prawnych istotnych w zakresie przetwarzania danych osobowych.

§ 2. SŁOWNIK TERMINÓW

Na potrzeby niniejszej Polityki, a także Załączników, wskazanym poniżej terminom nadaje się następujące znaczenie, uwzględniając przy tym znaczenia terminów zawartych w Rozporządzeniu Ogólnym:

1) **„Inspektor Ochrony Danych", „IOD" -** osoba wyznaczona przez Administratora danych osobowych do pełnienia funkcji Inspektora Ochrony Danych, która sprawuje nadzór nad przestrzeganiem zasad ochrony wynikających z Rozporządzenia Ogólnego, a w szczególności art. 5 Rozporządzenia Ogólnego i zobowiązana jest prowadzić dokumentację wynikającą z przepisów Rozporządzenia Ogólnego, Ustawy, rozporządzeń wykonawczych oraz niniejszej Polityki,
2) **„Administrator danych osobowych"**, „**Administrator**", „**ADO**" – Opolski Związek Tenisa Stołowego z siedzibą przy ul. Damrota 6, 45-064 Opole, wpisanym do rejestru stowarzyszeń, Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Opola-Ozimskiej w Opolu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000227352, NIP: 754-26-49-568, REGON: 531624100,
3) „**Dane osobowe**", „**Dane**" – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość,
4) „**Dane szczególnych kategorii**" - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne oraz dane dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby,
5) „**Osoba, której dane dotyczą**" – każda osoba fizyczna, bez względu na jej obywatelstwo, wiek czy też zdolność do czynności prawnych, której dane osobowe są przetwarzane,
6) „**Przetwarzanie danych osobowych**", „**Przetwarzanie danych**", „**Przetwarzanie**" – każda operacja lub zestaw operacji dokonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, jak np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
7) **„Ustawa**" – ustawa z dnia 26.05.2018 roku o ochronie danych osobowych,
8) **„Rozporządzenie Ogólne"** - 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,
9) „**Zbiór danych osobowych**", „**Zbiór danych"**, „**Zbiór**" – każdy uporządkowany zestaw Danych osobowych, dostępnych według określonych kryteriów, scentralizowanych, zdecentralizowanych lub rozproszonych funkcjonalnie lub geograficznie. Zbiór danych może być prowadzony zarówno w formie elektronicznej jak i papierowej,

10) „**Pseudonimizacja**” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
11) „**Profilowanie**” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,
12) „**Podmiot przetwarzający**” lub „**Procesor**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,
13) „**Zgoda**” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych,
14) „**Naruszenie ochrony danych osobowych**” oznacza 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) „**Dane dotyczące zdrowia**” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia,
16) „**Organ Nadzorczy**” lub „**PUODO**” oznacza Prezesa Urzędu Ochrony Danych Osobowych,
17) „**Usługa Społeczeństwa Informacyjnego**” - każda usługa normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług.

§ 3. ZAKRES OBOWIĄZYWANIA POLITYKI

1. Celem niniejszej Polityki jest określenie zasad przetwarzania danych osobowych oraz ich bezpieczeństwa, jako zestaw praw, reguł, procedur i praktycznych rozwiązań regulujących sposób ich przetwarzania, zarządzania, ochrony i dystrybucji wewnątrz Związku, jak i w kontaktach z otoczeniem, a w szczególności z klientami i kontrahentami.

2. Polityka opisuje zabezpieczenia techniczne i organizacyjne zastosowane celem ochrony danych osobowych w Związku i stanowi podstawowy dokument dotyczący ochrony danych osobowych wewnątrz Związku.

3. Wszyscy pracownicy zatrudnieni w Związku, niezależnie od stosunku prawnego regulującego podstawę ich zatrudnienia, zobligowani są do zapoznania się i przestrzegania postanowień Polityki. Powyższe znajduje zastosowanie w szczególności do osób posiadających chociażby przejściowy dostęp do danych, niezależnych podwykonawców oraz osób, które realizują zadania w imieniu podwykonawców. Pracownicy składają do dokumentacji wewnętrznej Związku pisemne oświadczenia o zapoznaniu się z treścią Polityki (**Załącznik nr 10**)

4. Polityka obowiązuje w zakresie wszystkich operacji związanych z przetwarzaniem danych, niezależnie od formy i sposobu ich przetwarzania oraz tego kogo dane są przetwarzane.

5. Polityka znajduje zastosowanie do:
    1) danych osobowych przetwarzanych w systemach informatycznych oraz w tradycyjnej - papierowej formie, a także przechowywanych na wszelkich nośnikach magnetycznych, optycznych, elektronicznych takich jak: zewnętrzny dysk, dysk twardy, dyskietka, CD/DVD, pamięć masowa typu flash, a także w książkach i kartotekach ewidencyjnych,
    2) danych osobowych przetwarzanych zarówno w zbiorach danych, zestawach oraz pojedynczych informacjach osobowych,
    3) informacji dotyczących bezpieczeństwa danych osobowych, w szczególności informacji służących do uwierzytelnienia się w systemach informatycznych, w których mogą występować dane osobowe.

6. Polityka znajduje zastosowanie do wszystkich lokalizacji – budynków i pomieszczeń – w których są lub będą przetwarzane dane.

7. Wykaz lokalizacji, w których przetwarzane są dane osobowe stanowi **Załącznik nr 1**. IOD odpowiada za aktualizację Załącznika nr 1.

§ 4. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. Zapewnienie bezpieczeństwa danych polega na zagwarantowaniu:
    1) poufności danych – zapewnieniu, iż jedynie uprawnione jednostki posiadać będą dostęp do danych,
    2) integralności danych – zapewnieniu dokładności oraz kompletności danych, jak również metod i jednostek upoważnionych do ich przetwarzania,
    3) dostępności danych – zapewnieniu dostępu do danych osobom, których dane dotyczą,
    4) prawidłowego zarządzenia ryzykiem – szeregu działań zmierzających do umożliwienia zidentyfikowania, kontrolowania oraz eliminowania powstającego w związku z przetwarzaniem danych ryzyka,
    5) rozliczalności działań – zapewnieniu, iż wszystkie działania istotne w zakresie przetwarzania danych zostały zarejestrowane, a w konsekwencji możliwym jest zidentyfikowanie jednostki odpowiedzialnej za Przetwarzanie danych,

2. Celem zapewnienia bezpieczeństwa danych osobowych wprowadzono mechanizmy ochronne, które wzajemnie się przenikają. Mechanizmami tymi są zabezpieczenia fizyczne, środki sprzętowe, procedury organizacyjne, oprogramowanie systemowe.

3. Zabezpieczenia fizyczne obejmują w szczególności:
    1) całodobowy monitoring pomieszczeń, które uznane przez IOD są za kluczowe z perspektywy ochrony danych,
    2) zamykanie na klucz pomieszczeń, w których dokonuje się jakichkolwiek operacji związanych z przetwarzaniem danych. Klucze posiadają wyłącznie uprawnione osoby, których rejestr prowadzi IOD,
    3) przechowywanie fizycznych zbiorów danych w szafkach zamykanych na klucz,
    4) całodobowa ochrona wskazanych przez IOD lokalizacji przez wyspecjalizowane podmioty ochrony mienia,
    5) zamykanie na klucz szafek z segregatorami,
    6) zamykanie przenośnego sprzętu komputerowego w szafkach zamykanych na klucz lub sejfach,
    7) budynek zabezpieczony w system przeciwpożarowy,
    8) profesjonalny system antywłamaniowy.

4. Środki sprzętowe obejmują zwłaszcza:
    1) typ i standard sprzętu wykorzystywanego w ramach systemu informatycznego służącego do przetwarzania danych osobowych (komputery, sieci, routery), zapewniający odpowiednie restrykcje w zakresie dostępu do danych,
    2) odpowiednie zabezpieczanie teletransmisji danych,
    3) indywidualne karty wstępu do lokalizacji, w których następuje przetwarzanie danych (identyfikatory),
    4) zabezpieczenia wejścia do komputera i aplikacji zawierających dane osobowe hasłem.

5. Procedury organizacyjne obejmują w szczególności:
    1) szkolenia dla pracowników mających dostęp do danych,
    2) audyty ochrony danych osobowych prowadzone minimum raz na 2 lata,
    3) obowiązek IOD do dokładania ciągłych starań mających na celu zapewnienie zgodności ochrony danych z aktualnie obowiązującymi wymaganiami,
    4) obowiązek wykonywania przez IOD innych obowiązków nałożonych na niego Polityką,
    5) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,
    6) uwzględnianie ochrony danych osobowych już na etapie projektowania nowej usługi, towaru lub realizacji nowego projektu w ramach Związku (konsultacje z IOD),
    7) nadawanie upoważnień do przetwarzanie danych osobowych pracownikom odpowiednio do zakresu powierzonych im obowiązków,
    8) każdorazowe notyfikowanie wyniesienia dokumentów / nośników zawierających dane osobowe poza siedzibę podmiotu,
    9) przeprowadzanie spotkań w wydzielonych pomieszczeniach, niedostępnych dla osób postronnych,
    10) zapoznanie pracowników mających dostęp do danych osobowych z powszechnie obowiązującymi przepisami z zakresu ochrony danych osobowych oraz wewnętrznymi uregulowaniami Związku (Oświadczenie stanowi **Załącznik nr 10**).

6. Środki ochrony w ramach systemowych narzędzi programowych:
    1) ograniczenie identyfikatorem i hasłem dostępu do urządzeń za pomocą których przetwarzane są dane, a także hasłem do programów,
    2) szyfrowanie przesyłanych danych,
    3) anonimizacja/pseudonimizacja danych osobowych,
    4) stosowanie stopniowalnych uprawnień,
    5) wymuszenia zmiany haseł,
    6) systemowe wprowadzanie dat wprowadzania danych,
    7) wygaszacze ekranu,
    8) ograniczanie dostępu użytkownika jedynie do konkretnych zasobów poprzez wprowadzenie systemu użytkowników i haseł, ograniczenie dostępu do poziomu poleceń systemowych, rejestrację nieudanych logowań do systemu,
    9) stała opieka informatyczna nad serwerem Związku,
    10) na stanowiskach, które są podłączone do sieci zewnętrznej - wykaz zastosowanych środków ochrony, w tym wykaz programów antywirusowych.

7. Organizacja pracy przy przetwarzaniu danych oraz zasady przetwarzania:
    1) przetwarzanie danych przez pracowników Związku odbywać się będzie jedynie po zapoznaniu ich z wszelkimi dokumentami obowiązującymi w Związku dotyczącymi ochrony danych oraz po przyznaniu stosownego upoważnienia do przetwarzania tych danych. Upoważnienia może przyznawać osoba posiadająca pełnomocnictwo wydane przez IOD. Wzór upoważnienia określa **Załącznik nr 2**,

2) wykaz osób uprawnionych do przetwarzania danych osobowych w Związku znajduje się u IOD,
3) osoba przetwarzająca dane, w czasie ich przetwarzania, jest odpowiedzialna za ich bezpieczeństwo i w tym celu powinna ona dokładać wszelkich starań celem uniemożliwienia wglądu, bądź zmiany przetwarzanych danych, przez osoby do tego nieupoważnione,
4) w czasie przetwarzania danych, osoba przetwarzająca dane powinna dokładać wszelkich starań celem uniemożliwienia wglądu, bądź zmiany przetwarzanych danych, przez osoby do tego nieupoważnione, osoby upoważnione do przetwarzania danych osobowych, zobowiązane są do przestrzegania zasad, dotyczących wprowadzania osób trzecich do obszaru przetwarzania danych osobowych. Ruch osób z zewnątrz w wymienionym obszarze powinien odbywać się pod kontrolą osób upoważnionych,
5) budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych.

8. Naruszeniem zasad ochrony danych osobowych jest w szczególności:
    1) nieuprawniony dostęp lub próba dostępu do danych,
    2) udostępnianie danych osobom nieupoważnionym,
    3) przetwarzanie danych przez osoby nieuprawnione,
    4) utrata danych zapisanych na kopiach zapasowych,
    5) naruszenie poufności, integralności lub dostępności danych.

§ 5. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Wszystkie dane osobowe gromadzone w Związku mogą być przetwarzane wyłącznie w sposób zgodny z prawem, rzetelnie i w sposób przejrzysty dla osób, których dane dotyczą („**zgodność z prawem, rzetelność i przejrzystość**").

2. Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („**ograniczanie celu**").

3. Przetwarzane Dane osobowe musza być prawidłowe i w razie potrzeby uaktualniane. Należy podejmować wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle ochrony celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („**prawidłowość**").

4. Dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („**ograniczenie przechowywania**").

5. Dane osobowe są przetwarzane przez Związek 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 („**integralność i poufność**").

6. Związek jest odpowiedzialny za przestrzeganie zasad, o których mowa w paragrafie 5 ust. 1-5 powyżej i musi być w stanie wykazać ich przestrzeganie („**rozliczalność**").

7. W przypadku zbierania danych osobowych bezpośrednio od osób - na formularzach, umowach, kwestionariuszach, drukach, zarówno papierowych, jak i elektronicznych, należy umieszczać na nich klauzulę informacyjną dotyczącą przetwarzania danych osobowych.

8. Klauzula informacyjna zawiera:
    1) pełną nazwę i adres Związku tj. Administratora Danych Osobowych oraz dane kontaktowe do Związku;
    2) dane kontaktowe IOD;
    3) cel przetwarzania danych oraz podstawę prawną przetwarzania;
    4) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe kryteria ustalania tego okresu;
    5) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
    6) jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą (art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) Rozporządzenia Ogólnego) – informacje o prawie do

cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

7) nazwy podmiotów, którym dane mogą być udostępniane;
8) informacje o prawie wniesienia skargi do Organu Nadzorczego;
9) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
10) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

9. W sytuacji, gdy podanie danych jest obowiązkowe, należy wskazać przepis prawa, umożliwiający przetwarzanie danych bez zgody osoby, której dane dotyczą.

10. Jeżeli Związek planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.

§ 6. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

Prawo dostępu do informacji

1. Każda osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
   a) cele przetwarzania;
   b) kategorie odnośnych danych osobowych;
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   e) informacje o prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f) informacje o prawie wniesienia skargi do organu nadzorczego;
   g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
   h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

   Ponadto, Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną

2. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych lub kopii danych osobowych na pisemny lub elektroniczny (e-mail) wniosek pochodzący od osoby, której dane dotyczą, odpowiedź musi nastąpić w terminie 7 (słownie: siedem) dni od daty jego otrzymania.

3. Na wniosek osoby, której dane dotyczą informacji, o których mowa w ust. 1 udziela na piśmie lub w formie elektronicznej (e-mail) Inspektor Danych Osobowych. Odpowiedzi w formie elektronicznej można udzielić wyłącznie, gdy wniosek osoby, której dane dotyczą został złożony w takiej formie.

4. IOD lub osoba upoważniona przez IDO prowadzi rejestr wniosków i udostępnień informacji o przetwarzanych danych osobowych oraz kopii danych osobom, których one dotyczą, zgodnie ze wzorem zawartym w **Załączniku nr 6**.

Prawo do sprostowania danych

5. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Prawo do usunięcia danych („prawo do bycia zapomnianym")

6. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
    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, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą;
    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 Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator;
    f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

7. Jeżeli Administrator upublicznił dane osobowe, a na mocy ust. 6 powyżej ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

8. Ust. 6 i 7 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
    a) do korzystania z prawa do wolności wypowiedzi i informacji;
    b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
    e) do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do ograniczenia przetwarzania danych

9. Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania w następujących przypadkach:
    a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;
    b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
    c) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
    d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

10. Jeżeli na mocy ust. 9 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej.

11. Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

Prawo do przenoszenia danych

12. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:
    a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy; oraz
    b) przetwarzanie odbywa się w sposób zautomatyzowany.

13. Wykonując prawo do przenoszenia danych na mocy ust. 12, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi (nie Związkowi), o ile jest to technicznie możliwe.

Prawo do sprzeciwu

14. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na:

a) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
b) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

- w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

15. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

16. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

17. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie do sprzeciwu, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

18. osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

Prawo nie podlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu

19. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Powyższe nie ma zastosowania, jeżeli ta decyzja:
    a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a Administratorem;

    b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
    c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

20. W przypadkach, o których mowa w ust. 19 lit. a) i c), Administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

21. Decyzje, o których mowa w ust. 19 lit. a)-c), nie mogą opierać się na szczególnych kategoriach danych osobowych, chyba że przetwarzanie odbywa się na podstawie:
    - wyraźnej zgody osoby, której dane są przetwarzane;
    - przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

    -i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Procedura realizacji praw przez osoby, których dane są przetwarzane

15. W sytuacji wniesienia przez osobę:
    - wniosku o sprostowanie danych
    - żądania skorzystania z prawa do bycia zapomnianym;
    - żądania skorzystania z prawa do ograniczenia przetwarzania;
    - żądania skorzystania z prawa do przeniesienia danych;
    - złożenia sprzeciwu wobec przetwarzania danych;
    - żądania skorzystania z prawa nie podlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu;

    informacja o wniesieniu wniosku, sprzeciwu lub żądania przekazywana jest do IOD, który ocenia zasadność otrzymanego wniosku.

16. W sytuacji, gdy wniosek, sprzeciw lub żądanie jest zasadne, IOD podejmuje adekwatne działania i niezwłocznie doprowadza do realizacji prawa osoby, której dane są przetwarzane oraz informuje ją o podjętych działaniach w terminie 7 dni od dnia otrzymania wniosku, sprzeciwu lub żądania. Informację zwrotną przekazuje się w formie:
    - pisemnej,
    - pisemnej lub elektronicznej (e-mail) jeżeli wniosek, sprzeciw lub żądanie było złożone w formie elektronicznej.

17. W razie odmowy uwzględnienia wniosku, sprzeciwu lub żądania IOD w terminie 7 (słownie: siedem) dni od dnia otrzymania wniosku, sprzeciwu lub żądania informuje o wnioskodawcę o odmowie wraz z uzasadnieniem, w tym wskazując podstawę prawną odmowy. Odmowy wraz z uzasadnieniem udziela się w formie:
    - pisemnej,

- pisemnej lub elektronicznej (e-mail) jeżeli wniosek, sprzeciw lub żądanie było złożone w formie elektronicznej.

18. IOD lub osoba upoważniona przez ADO prowadzi rejestr wniosków, sprzeciwów i żądań, zgodnie ze wzorem zawartym w **Załączniku nr 6**.

§ 7. ZADANIA OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH

1. Za bezpieczeństwo danych odpowiadają:
    1) Inspektor Ochrony Danych (**IOD**),
    2) Administrator Sieci Informatycznej (**ASI**),
    3) pracownicy upoważnieni do przetwarzania danych osobowych.

2. Zadania IOD obejmują:
    1) tworzenie, wdrażanie, administrowanie i interpretowanie Polityki, standardów, zaleceń oraz procedur, dotyczących przetwarzania danych osobowych,
    2) koordynowanie działań w zakresie ochrony danych osobowych,
    3) czuwanie nad zapewnieniem przestrzegania przepisów prawa w zakresie danych osobowych,
    4) ścisła współpraca z ASI w zakresie ustalenia zasad i nadzoru nad poprawnością przetwarzania danych osobowych w systemach informatycznych,
    5) prowadzenia wykazu lokalizacji, w których przetwarzane są dane osobowe, zgodnie z **Załącznikiem nr 1**,
    6) zapoznanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami o ochronie danych osobowych poprzez przeprowadzenie szkoleń,
    7) prowadzenie rejestru czynności przetwarzania danych, zgodnie z **Załącznikiem nr 3** oraz prowadzenie rejestru wszystkich kategorii czynności przetwarzania danych, zgodnie z **Załącznikiem nr 9**,
    8) wydawanie, na podstawie pełnomocnictwa ADO, upoważnień do przetwarzania danych pracownikom Związku oraz osobom mającym wykonywać dla Związku czynności związane z dostępem do danych osobowych, w tym w ramach umów powierzenia przetwarzania danych osobowych zawartych przez Związek z podmiotem trzecim,
    9) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, zgodnie z **Załącznikiem nr 5**,
    10) prowadzenie ewidencji podmiotów przetwarzających, zgodnie z **Załącznikiem nr 11**,
    11) przeciwdziałanie dostępowi do danych osobowych osób niepowołanych do przetwarzania danych osobowych,
    12) sprawowanie kontroli nad danymi osobowymi wprowadzanymi do zbiorów,
    13) opiniowanie i akceptowanie umów dotyczących powierzenia innym podmiotom przetwarzania danych osobowych,
    14) kontrolowania przebiegu udostępniania danych osobowych oraz prowadzenie rejestrów udostępnień danych osobowych innym podmiotom, zgodnie z **Załącznikiem nr 6**,
    15) prowadzenie rejestru zdarzeń dotyczących naruszenia danych osobowych, zgodnie z **Załącznikiem nr 8**,
    16) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń,

17) sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń, na których zapisane są dane osobowe,
18) sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,
19) sprawowanie nadzoru nad prawidłowością archiwizacji, oraz usuwania danych osobowych,
20) monitorowanie wdrożonych zabezpieczeń,
21) przygotowywanie planu sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych na okres nie dłuższy niż rok, a nie krótszy niż kwartał, który obejmuje przynajmniej jedno sprawozdanie ze sprawdzeń, które ABI przekazuje ADO.

3. Zadania ASI obejmują:
    1) rejestrowanie i wyrejestrowywanie użytkowników systemu na podstawie wniosku,
    2) dokonywanie zmiany uprawnień użytkowników systemu na podstawie wniosku zaakceptowanego przez kierownika jednostki organizacyjnej,
    3) prowadzenie wykazu systemów informatycznych, w których przetwarzane są dane osobowe, zgodnie z **Załącznikiem nr 4** oraz ewidencji nośników informatycznych, zgodnie z **Załącznikiem nr 12**,
    4) przestrzeganie opracowanych dla systemu procedur bezpieczeństwa,
    5) utrzymanie systemu w sprawności technicznej w stopniu określonym w dokumentacji powykonawczej,
    6) przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe,
    7) konfigurowanie urządzeń i oprogramowania wg zapotrzebowania,
    8) aktualizowanie i konfigurowanie oprogramowania antywirusowego,
    9) reagowanie na naruszenia bezpieczeństwa i usuwanie ich skutków,
    10) nadzorowanie właściwego użytkowania oraz serwisowania urządzeń i oprogramowania zgodnie z zapisami Polityki,
    11) prowadzenie dziennika pracy systemu, który zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego w szczególności w przypadku awarii – opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski,
    12) w przypadku konserwacji systemu – opis podjętych działań, wnioski,
    13) wykonywanie kopii bezpieczeństwa informatycznych baz danych osobowych oraz systemów informatycznych,
    14) prowadzenie dokumentacji technicznej systemu – wielobranżowy opis środowiska pracy systemu,
    15) informowanie IOD o wszelkich zdarzeniach związanych lub mogących mieć wpływ na bezpieczeństwo systemu teleinformatycznego.

4. Pracownicy, niezależnie od stosunku prawnego regulującego podstawę ich zatrudnienia, zobowiązani są do:

1) zachowania w tajemnicy danych osobowych, do których mają dostęp, a także sposobów zabezpieczenia tych danych, zarówno w trakcie jak i po ustaniu zatrudnienia,
2) przestrzegania przepisów wewnętrznych obowiązujących w Związku wiążących się z ochroną danych osobowych,
3) zgłaszania zauważonych incydentów bezpieczeństwa związanych z ochroną danych osobowych,

w tym celu każda osoba zatrudniona w Związku, niezależnie od stosunku prawnego regulującego podstawę jego zatrudnienia, podpisuje oświadczenie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych wraz z oświadczeniem o zobowiązaniu do zachowania poufności, zgodnie z **Załącznikiem nr 10**.

§ 8. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH I REJESTRU WSZYSTKICH KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. IOD realizując Politykę sprawuje nadzór nad rodzajami oraz zawartością zbiorów danych osobowych.

2. IOD prowadzi rejestr czynności przetwarzania danych osobowych oraz rejestr wszystkich kategorii czynności przetwarzania danych osobowych w formie pisemnej, w tym elektronicznej, wedle **Załącznika nr 3 i nr 9**.

3. W rejestrze czynności przetwarzania znajdują się następujące informacje:
    a) Imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich w spół-administratorów, a także Inspektora Ochrony Danych;
    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) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
    f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
    g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

4. W rejestrze kategorii czynności przetwarzania znajdują się następujące informacje:
    a) Imię i nazwisko lub nazwa i dane kontaktowe Związku oraz każdego administratora, w imieniu którego działa Związek, a także inspektora ochrony danych osobowych danego administratora i Związku,
    b) Kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
    c) Gdy ma to zastosowanie – informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń,
    d) Jeśli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.
5. W rejestrach podaje się także datę ostatniej aktualizacji informacji dotyczących każdego zbioru danych.

6. Zabronione jest tworzenie zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych niż niezbędne dla realizacji celów, w których dane były gromadzone.

7. Każdy nowo powstały zbiór danych osobowych wymaga zgłoszenia do IOD. Osoba tworząca zbiór jest odpowiedzialna za dokonanie zgłoszenia.

§ 9. UDOSTĘPNIENIE, POWIERZENIE DANYCH OSOBOWYCH PODMIOTOM ZEWNĘTRZNYM

1. Powierzenie danych osobowych innemu podmiotowi zewnętrznemu, nieposiadającemu delegacji ustawowej do przetwarzania określonych danych osobowych, tj. z wyłączeniem podmiotów uprawnionych do otrzymania danych osobowych na mocy przepisów prawa w tym zwłaszcza przepisów Rozporządzenia Ogólnego, wymaga zawarcia umowy w formie pisemnej, określającej cel, zakres, warunki przetwarzania danych oraz sposób ich zabezpieczenia. Kopię umowy należy przekazać do IOD, który prowadzić będzie stosowny na tę okoliczność rejestr umów.

2. Przykładowe postanowienia klauzuli o powierzeniu przetwarzania danych osobowych wskazane zostały w **Załączniku nr 7**.

3. Dane osobowe udostępnia się podmiotom uprawnionym na podstawie przepisów prawa, na pisemny umotywowany wniosek, chyba że istnieją przepisy stanowiące inaczej. IOD prowadzi rejestr udostępnień danych osobowych innym podmiotom, którego wzór został określony w **Załączniku nr 6**.

§ 10. POSTĘPOWANIE Z INCYDENTAMI

1. Każdy pracownik Związku, niezależnie od stosunku prawnego regulującego podstawę jego zatrudnienia, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować o tym bezpośredniego przełożonego lub IOD.

2. W przypadku stwierdzenia incydentu (naruszenia), IOD prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   2) zabezpiecza ewentualne dowody,
   3) ustala osoby odpowiedzialne za naruszenie,
   4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   5) inicjuje działania dyscyplinarne,
   6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   7) dokumentuje prowadzone postępowania,
   8) sporządza raport i przekazuje do ADO.

3. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

4. Zgłoszenie, o którym mowa w ust. 3, musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

   Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki

5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

6. Zawiadomienie, o którym mowa w ust. 5 niniejszego paragrafu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w ust. 4 lit. b), c) i d) niniejszego paragrafu.

7. Zawiadomienie, o którym mowa w ust. 5 powyżej, nie jest wymagane, w następujących przypadkach:

a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

8. IOD prowadzi rejestr zdarzeń dotyczących naruszenia ochrony danych osobowych, zgodnie z **Załącznikiem nr 8**.

§ 11. PROCEDURA NISZCZENIA DANYCH OSOBOWYCH

1. Rozporządzenie Ogólne nakłada na podmioty zobowiązane do jego stosowania obowiązek przetwarzania danych osobowych zgodnie z zasadą ograniczenia przechowywania danych określoną w art. 5 ust. 1 lit. e) Rozporządzenia Ogólnego oraz w celu realizacji prawa do usunięcia danych osobowych („prawo do bycia zapomnianym") wprowadza się wskazane poniżej procedury niszczenia danych osobowych.
2. Niszczenie całości zbiorów danych osobowych ujawnionych w rejestrze czynności przetwarzania następuje wyłącznie na wniosek Administratora bądź IOD.
3. Sposób niszczenia danych osobowych musi być odpowiednio dobrany do rodzaju nośnika danych oraz ich kategorii.
4. Niszczenie danych osobowych polega na:
   a) Trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod,
   b) Anonimizacji danych osobowych, polegającej na pozbawieniu danych osobowych cech umożliwiających identyfikację osoby fizycznej, której dane dotyczą.
5. Niszczenie dokumentacji tradycyjnej (wydruki, notatki, dokumenty) odbywa się poprzez stosowanie anonimizacji bądź fizycznym zniszczeniu w niszczarce.
6. Procedura niszczenia nośników informatycznych odbywa się w zależności od rodzaju danego nośnika:
   a) Nośniki optyczne (płyty CD/DVD/BLU-RAY) – niszczenie odbywa się poprzez fizyczne przecięcie nośnika optycznego bądź fizyczne zniszczenie w niszczarce specjalnego przeznaczenia do tego typu nośników,
   b) Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) - niszczenie odbywa się poprzez elektroniczne usunięcie danych z nośnika bądź trwałe fizyczne zniszczenie sprzętowe powodujące brak możliwości ponownego odzyskania danych,
   c) Nośniki magnetyczne (dyskietki, dyski twarde HDD) - niszczenie odbywa się poprzez elektroniczne usunięcie danych z nośnika , trwałe fizyczne zniszczenie sprzętowe powodujące brak możliwości ponownego odzyskania danych bądź demagnetyzację nośnika.
7. W procedurze niszczenia całości zbioru danych osobowych ujawnionego w rejestrze czynności przetwarzania wymagana jest obowiązkowa obecność IOD. Zniszczenie całości zbioru danych osobowych ujawnionego w rejestrze czynności przetwarzania potwierdzone jest spisaniem protokołu, zgodnie z **Załącznikiem nr 13.**

§ 12. ODPOWIEDZIALNOŚĆ

8. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi, określonymi w Ustawie.

9. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w pkt 1, naruszenie zasad ochrony danych osobowych, obowiązujących w Związku, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

ZAŁĄCZNIK NR 1. Wykaz lokalizacji, w których następuje Przetwarzanie danych

Lp.	Lokalizacja – adres budynku oraz piętro	Nr pokoju	Funkcja lokalizacji [(1)]	Zabezpieczenie fizyczne [(2)]
1.	Budynek PSP nr1, ul. Kozielska 34, 47-100 Strzelce Op.		A	
2.	Kancelaria Podatkowa Forbis Krzysztof Kowalczuk, Krakowska 49, 47-100, Strzelce Op.		U	
3.				
4.				
5.				
6.				
7.				
8.				
9.				

[(1)] (S) - serwer, (K) - miejsce przechowywania kopii bezpieczeństwa, (Z) - pomieszczenie, w którym wykonywane są kopie bezpieczeństwa, (U) - pomieszczenie osób wprowadzających dane, (A) - pomieszczenie administratora bazy danych.

[(2)] (O) - kraty w oknach, (A) - alarm, (W) - wzmocnione drzwi.

ZAŁĄCZNIK NR 2. Upoważnienie do przetwarzania danych

Strzelce Op., dnia _____

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr ____

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz. Urz. UE L 119, s. 1) – dalej RODO – nadaję upoważnienie Pani/Pani:

_____

Imię i nazwisko

zatrudnionego/ną na stanowisku _____ do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.

Zakres, kategoria danych, które może przetwarzać określona upoważniona osoba lub rodzaj czynności, lub operacji, jakich może dokonywać na danych osobowych:
_____
_____
_____

Upoważnienie wydano w dniu _____

Upoważnienie traci ważność z dniem rozwiązania umowy o pracę lub odwołaniem upoważnienia.

Nr identyfikatora _____

/jeżeli dane przetwarzane są w systemie informatycznym/

Jednocześnie zobowiązuję Pana/Panią do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia 26.05.2018 r. o ochronie danych osobowych, Kodeksu pracy, a także polityką ochrony danych osobowych Opolskiego Związku Tenisa Stołowego.

Jednocześnie upoważniam Pana/Panią do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Opolskiego Związku Tenisa Stołowego.

Okres ważności

Od: _____

Do: _____

Inspektor Ochrony Danych

_____

Data i podpis

Data wygaśnięcia* _____

Odwołano, dnia _____

_____

Data i podpis osoby uprawnionej do odwołania upoważnienia

**data rozwiązania stosunku pracy/umowy cywilnoprawnej*

ZAŁĄCZNIK NR 3. Rejestr czynności przetwarzania danych osobowych

										Kategorie odbiorców						
Lp.	**Data utworzenia wpisu**	**Nazwa czynności przetwarzania**	**Administrator (nazwa i dane kontaktowe)**	**Inspektor ochrony danych (imię i nazwisko, dane kontaktowe)**	**Cele przetwarzania**	**Sposób zbierania danych**	**Kategorie osób, których dane dotyczą**	**Kategorie danych osobowych**	**Planowane terminy usunięcia danych**	**Inni administratorzy**	**Podmioty przetwarzające**	**Instytucje publiczne**	**Informacja o przekazaniu danych do państw trzecich**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**	**Podstawa prawna przetwarzania danych**	**Osoba dodająca wpis (imię i nazwisko)**
1.																
2.																
3.																

ZAŁĄCZNIK NR 4. Wzór wykazu systemów informatycznych, w których przetwarzane są dane osobowe

Nazwa systemu, aplikacji	Przeznaczenie systemu	Środowisko pracy –platforma systemowa i bazodanowa	Rodzaj przetwarzanych danych (zakres danych)	Komórki organizacyjne korzystające z systemu	Możliwość przyznawania indywidualnych identyfikatorów	Możliwość gradacji uprawnień*	Możliwość wymuszania zmiany i kontrola trywialności haseł*	Inne systemy, z którymi system się komunikuje i wymienia dane	Właściciel (Związek), firma zewnętrzna- outsour.)	Lokalizacja bazy danych/serwera	Odnotowanie daty pierwszego wprowadzenia danych osobowych do systemu	Odnotowanie identyfikatora Użytkownika przetwarzającego dane osobowe wprowadzającego dane	Możliwość odnotowania sprzeciwu określonego w art. 32 ust. 1 pkt 8 u.o.d.o	Możliwość odnotowania źródła danych, w przypadku zbierania danych nie od osoby, której dane dotyczą	Możliwość odnotowania informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia	Możliwość sporządzenia i wydrukowania raportu zawierającego dane osobowe wraz z informacjami z KOLUMN 12-16
1	2	3	4	5	6*	7*	8*	9	10	11	12*	13*	14*	15*	16*	17*

W kolumnach 6 – 8 oraz 12-17 podać odpowiedzi: TAK, NIE, NIE DOTYCZY

ZAŁĄCZNIK NR 5. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Stanowisko/ jednostka/ komórka organizacyjna	Numer upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Identyfikator w danym systemie informatycznym
1.							
2.							
3.							
4.							
5.							
6.							

ZAŁĄCZNIK NR 6. Wzory dotyczące rejestrów udostępnień danych osobowych oraz sprzeciwów na przetwarzanie danych

Wzór Rejestru wniosków i udostępnień kopii danych oraz informacji o przetwarzanych danych osobowych osobom, których one dotyczą:

L.p.	Data wpłynięcia wniosku od osoby	Imię i nazwisko osoby wnioskującej	Data udostępnienia	Rodzaj zbioru/zasobu i jego lokalizacja

Wzór Rejestru sprzeciwów, żądań skorzystania z prawa oraz wniosków o realizację praw od osób, których one dotyczą:

L.p.	Data wpłynięcia wniosku, żądania lub sprzeciwu	Imię i nazwisko osoby wnioskującej	Rodzaj wniosku, żądania lub sprzeciw	Decyzja dotycząca wniosku	Data wykonania decyzji	Rodzaj zbioru/zasobu i jego lokalizacja

ZAŁĄCZNIK NR 7. Wzór postanowień dotyczących powierzenia czynności przetwarzania danych osobowych do umowy zlecenia usługi

§…

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „**Rozporządzeniem**") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§…

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie Umowy dane _____, będących danymi zwykłymi w postaci _____
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu _____.

§…

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby,

której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 48 h.

§…

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3 - dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§…

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§…

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiejkolwiek decyzji

administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych (Prezesa Urzędu Ochrony Danych Osobowych). Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§…

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* od ….. do ….. .*
2. Każda ze stron może wypowiedzieć niniejszą Umowę z zachowaniem 1-miesięcznego okresu wypowiedzenia.

§…

Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
b) przetwarza dane osobowe w sposób niezgodny z Umową;
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§…

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („**dane poufne**”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

ZAŁĄCZNIK NR 8. Wzór rejestru zdarzeń, dotyczących naruszenia ochrony danych

Rejestr Naruszeń Ochrony Danych Osobowych															
L.p.	Naruszenie (stypizowany opis naruszenia)	Data i godzina zgłoszenia naruszenia	Data naruszenia/okres, którego dotyczy	Kategorie i liczba osób, których dotyczy naruszenie	Zakres danych i/lub kategorie danych, których dotyczy naruszenie	Osoba / źródło informacji o zdarzeniu	Miejsce naruszenia	Okoliczności naruszenia – opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia	Opis skutków/ konsekwencji naruszenia	Osoba/ jednostka odpowiedzialna za naruszenie	Podjęte działania/opis środków zastosowanych lub proponowanych do	Rezultat działań naprawczych	Osoba odpowiedzialna za wdrożenie działań naprawczych	Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy	Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych (jeśli tak: data i godzina zgłoszenia)
1.															
2.															
3.															
4.															
5.															
6.															
7.															
8.															

ZAŁĄCZNIK NR 9. Wzór rejestru wszystkich kategorii czynności przetwarzania

Rejestr wszystkich kategorii czynności przetwarzania						
L.p.	**Nazwa powierzonego procesu**	**Nazwa i dane kontaktowe administratora, który powierzył przetwarzanie danych**	**Departament przetwarzającego odpowiedzialny za przetwarzanie**	**Kategorie przetwarzań dokonywanych w imieniu administratora**	**Opis technicznych i organizacyjnych środków bezpieczeństwa**	**Informacja o przekazaniu danych osobowych do państwa trzeciego**
1.						
2.						
3.						
4.						
5.						
6.						

ZAŁĄCZNIK NR 10. Wzór oświadczenia o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych oraz oświadczenie o zobowiązaniu do zachowania poufności

Wrocław, dnia _____

Oświadczenie o zachowaniu poufności i zobowiązaniu do przestrzegania przepisów w zakresie ochrony danych osobowych

Ja niżej podpisany/-a _____ zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których zostanie przyznany mi dostęp w związku z wykonywaniem na rzecz Opolskiego Związku Tenisa Stołowego z siedzibą we Opolu ul. Damrota 6, 45-064, numer KRS: 0000227352 (dalej: **Związek**) zadań wynikających z:

Umowy o pracę / umowy cywilno-prawnej / stażu / praktyki / stosunku członkostwa w organach* zarówno w trakcie jej trwania, jak i po jej ustaniu.

Zobowiązuję się do przestrzegania regulacji wewnętrznych obowiązujących w Związku dotyczących ochrony danych osobowych określonych w:

1. Polityce bezpieczeństwa danych osobowych.

Oświadczam, iż poinformowano mnie o podstawach prawnych ochrony danych osobowych, które stanowią:

1. 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,
2. Ustawa o ochronie danych osobowych z dnia 26.05. 2018 r.

oraz o wynikającej z nich odpowiedzialności pracowniczej i cywilnoprawnej, w szczególności iż naruszenie zasad ochrony danych osobowych może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

_____

Podpis osoby składającej oświadczenie

*niepotrzebne skreślić

ZAŁĄCZNIK NR 11. Wzór ewidencji podmiotów przetwarzających

Ewidencja podmiotów przetwarzających							
L.p.	**Nazwa i adres podmiotu przetwarzającego**	**Adres podmiotu przetwarzającego**	**Imię i nazwisko oraz telefon i adres e-mail do osoby kontaktowej do podmiotu przetwarzającego**	**Numer umowy o powierzenie przetwarzania danych osobowych i data jej zawarcia**	**Czas obowiązywania umowy**	**Rodzaj zbioru danych osobowych i jego lokalizacja**	**Kategorie danych, których dotyczy udostępnienie**
1.							
2.							
3.							
4.							
5.							

ZAŁĄCZNIK NR 12. Wykaz elektronicznych nośników informacji zawierających danych osobowych

Wykaz elektronicznych nośników informacji zawierających dane osobowe					
L.p.	**Rodzaj nośnika**	**Model**	**Rodzaj zbioru danych osobowych przechowywanych na nośniku**	**Kategorie danych osobowych**	**Osoby mające dostęp do nośnika**
1.					
2.					
3.					
4.					

ZAŁĄCZNIK NR 13. Wzór protokołu zniszczenia zbioru danych osobowych ujawnionego w rejestrze czynności przetwarzania

PROTOKÓŁ ZNISZCZENIA ZBIORU DANYCH OSOBOWYCH

1. Data operacji:_____
2. Miejsce operacji: _____
3. Nazwa zbioru danych osobowych: _____
4. W przypadku niszczenia kopii zapasowej, oznaczenie numeru niszczonej kopii zapasowej:_____
5. Rodzaj nośnika:_____
6. Sposób zniszczenia:_____
7. Osoby obecne w procedurze: _____
8. Protokół sporządził:
   Imię:_____
   Nazwisko:_____
   Stanowisko:_____