POLITYKA BEZPIECZEŃSTWA

UCZNIOWSKI KLUB SPORTOWY DĄB 19
NIP 634 250 32 91

Data i miejsce sporządzenia dokumentu:	Katowice 20.04.2018
Ilość stron:	14
Organ zatwierdzający:	Prezes Beata Golda

SPIS TREŚCI 2

1. WSTĘP

1.1. INFORMACJE OGÓLNE

Niniejszy dokument Polityki Bezpieczeństwa został opracowany przez Administratora Danych – UCZNIOWSKI KLUB SPORTOWY DĄB 19, w celu zapewnienia zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa.
Polityka Bezpieczeństwa oraz dokumenty w niej wskazane stanowią dokumentację przetwarzania danych osobowych w rozumieniu § 1 pkt 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.) oraz RODO Rozporządzenie o Ochronie Danych Osobowych wydane przez Parlament Europejski i Radę UE z 2016 roku dotyczące ochrony danych osób fizycznych odnośnie przetwarzania danych osobowych z 17 maja 2016 roku

Polityka Bezpieczeństwa obowiązuje od dnia 25 maja 2018 r.. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu Polityki Bezpieczeństwa, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.
Każda osoba mającą dostęp do danych osobowych z upoważnienia Administratora Danych, została zapoznana z Polityką Bezpieczeństwa i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Osoby o których mowa, złożyły na piśmie oświadczenie o zapoznaniu się z treścią Polityki Bezpieczeństwa oraz zobowiązały się do stosowania zawartych w niej postanowień.

1.2. CEL PRZYGOTOWANIA POLITYKI BEZPIECZEŃSTWA

Podstawowym celem przygotowania i wdrożenia dokumentu Polityki Bezpieczeństwa jest zapewnienie zgodności działania klubu z ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi w tym RODO. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:
1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.),

2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.),

3) RODO Rozporządzenie o Ochronie Danych Osobowych wydane przez Parlament Europejski i Radę UE z 2016 roku dotyczące ochrony danych osób fizycznych odnośnie przetwarzania danych osobowych z 17 maja 2016 roku

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem Polityki Bezpieczeństwa jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie

odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

1.3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz , odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Na Politykę Bezpieczeństwa składają się następujące informacje:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

3) sposób przepływu danych pomiędzy poszczególnymi systemami,

4) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczności przetwarzanych danych.

Politykę Bezpieczeństwa stosuje się do wszelkich czynności, stanowiących w myśl ustawy o ochronie danych osobowych, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie Polityki Bezpieczeństwa. Rygorowi Polityki Bezpieczeństwa podlegają także dane powierzone UCZNIOWSKI KLUB SPORTOWY DĄB 19 do przetwarzania na podstawie pisemnej umowy powierzenia przetwarzania danych osobowych oraz dane osobowe, których UCZNIOWSKI KLUB SPORTOWY DĄB 19 jest odbiorcą w rozumieniu ustawy o ochronie danych osobowych.

1.4. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1. **administrator danych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych, w niniejszej Polityce bezpieczeństwa zwany także UCZNIOWSKI KLUB SPORTOWY DĄB 19 lub klubem.

2. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

3. **hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

4. **identyfikator użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

5. **integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

6. **odbiorca danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

6.1. osoby, której dane dotyczą,

6.2. osoby upoważnionej do przetwarzania danych,

6.3. przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,

6.4. podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,

6.5. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

7. **państwo trzecie** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego,

8. **Polityka Bezpieczeństwa** – dokument polityki bezpieczeństwa w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „Polityką”,

9. **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

10. **przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

11. **raport** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

12. **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

13. **rozporządzenie** – rozumie się przez to rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.), oraz Rozporządzenie o Ochronie Danych Osobowych wydane przez Parlament Europejski i Radę UE z 2016 roku dotyczące ochrony danych osób fizycznych odnośnie przetwarzania danych osobowych z 17 maja 2016 roku zwane dalej RODO

15. **sieć publiczna** - rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2004. Nr 171, poz.1800 z późn. zm.),

16. **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2004. Nr 171, poz.1800 z późn. zm.),

18. **teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

19. **ustawa** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwaną dalej „Ustawą", wraz ze zmianami

20. **usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

21. **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

22. **zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

23. **zbiór danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

24. **zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, oraz Polityki odpowiadają w UCZNIOWSKI KLUB SPORTOWY DĄB 19 :

1. Administrator Danych,

2. Osoby Zarządzające Zbiorami Danych,

3. Każda osoba wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz i, która uzyskała upoważnienie do przetwarzania danych osobowych.

2.2. ADMINISTRATOR DANYCH

1. UCZNIOWSKI KLUB SPORTOWY DĄB 19 , reprezentowana przez prezesa,

2.3. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

klub nie powołuje ABI . Zgodnie z art. 36a ust. 1 u.o.d.o., powołanie ABI jest uprawnieniem, a nie obowiązkiem administratora danych. W przypadku niepowołania ABI, jego zadania wykonuje sam administrator danych (art. 36b u.o.d.o.).

2.4. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

klub nie powołuje ASI . Zgodnie z art. 36 ust. 1 u.o.d.o., powołanie ASI jest uprawnieniem, a nie obowiązkiem administratora danych. W przypadku niepowołania ASI, jego zadania wykonuje sam administrator danych (art. 36b u.o.d.o.).

2.5. OSOBY ZARZĄDZAJĄCE ZBIOREM DANYCH OSOBOWYCH

1. Zarządzającymi Zbiorami Danych Osobowych są osoby, które odpowiadają za bieżące zarządzanie poszczególnymi zbiorami danych osobowych przetwarzanymi w strukturze Administratora Danych, są nimi osoby wyznaczane pisemnie przez Administratora Bezpieczeństwa Informacji.

2. Dla każdego zbioru danych musi zostać wyznaczona jedna osoba pełniąca obowiązki Zarządzającego Zbiorem Danych Osobowych, przy czym możliwe jest pełnienie przez jedną osobę funkcji Zarządzającego Zbiorem Danych Osobowych w stosunku do kilku zbiorów danych osobowych.

3. Zarządzający Zbiorem Danych Osobowych jest zobowiązany do ścisłej współpracy z Administratorem Danych w zakresie przetwarzania danych osobowych w zarządzanym przez niego zbiorze danych, a w szczególności zobowiązany jest do wykonywania jego poleceń w dziedzinie bezpieczeństwa przetwarzania danych.

4. Do uprawnień i obowiązków Zarządzającego Zbiorem Danych Osobowych należą w szczególności:

4.1 zgłaszanie do Administratora Danych zamiaru zbierania danych osobowych i utworzenia zbioru, bądź jego nowego elementu (podzbioru) oraz konsultowanie kwestii zamiaru wprowadzenia w zbiorze zmian w zakresie: sposobu zbierania oraz udostępniania danych, celu i zakresu przetwarzania danych, miejsca przetwarzania danych, zmiany formy przetwarzania danych, zaprzestania przetwarzania, usunięcia danych ze zbioru lub zniszczenia zbioru danych oraz zastosowanych zabezpieczeń związanych z jego przetwarzaniem,

4.2 udzielanie Administratorowi Danych oraz innym pracownikom upoważnionym do przetwarzania danych osobowych w nadzorowanym przez niego zbiorze wyjaśnień w sprawie zarządzanych przez niego zbiorów oraz konsultowanie z nimi odpowiedzi na wszelkie zapytania w tej kwestii kierowane przez podmioty zewnętrzne,

4.3 nadawanie upoważnień osobom przetwarzającym dane osobowe w nadzorowanych przez nich zbiorach,

4.4 nadzór nad wdrożeniem i stosowaniem fizycznych środków zabezpieczenia obszarów, w których przetwarzane są dane osobowe zawarte w zbiorze, którym zarządza,

4.5 udział w wewnętrznym postępowaniu kontrolnym oraz w postępowaniu kontrolnym prowadzonym przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych w odniesieniu do zarządzanego przez niego zbioru,

4.6 inne czynności przewidziane w niniejszej Polityce oraz Instrukcji.

5. W przypadku zmiany stanowiska pracy lub długotrwałej przerwy w jej wykonywaniu przez osobę pełniącą funkcję Zarządzającego Zbiorem Danych Osobowych należy dokonać powołania innej osoby na jej miejsce w trybie określonym w punkcie 1 powyżej. Zarządzający Zbiorem Danych Osobowych musi dokonać przekazania swych obowiązków w odniesieniu do nadzorowanego zbioru. Poprzez zmianę stanowiska pracy należy rozumieć zmianę stanowiska pracy w ramach i jak i całkowite rozwiązanie stosunku pracy. Poprzez długotrwałą przerwę w wykonywaniu pracy należy rozumieć przebywanie pracownika na zwolnieniu lekarskim, urlopie bezpłatnym lub macierzyńskim przez okres powyżej 30 dni.

2.6. PRACOWNICY URZĘDU MIEJSKIEGO POSIADAJĄCY DOSTĘP DO DANYCH OSOBOWYCH

1. Każdy pracownik UCZNIOWSKI KLUB SPORTOWY DĄB 19 , który uzyskał upoważnienie do przetwarzania danych osobowych, zobowiązany jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki oraz Instrukcji.

2. Dostęp do określonego zbioru danych osobowych pracownik i uzyskuje na podstawie pisemnego upoważnienia, otrzymanego w trybie określonym w Rozdziale 3 niniejszej Polityki.

3. Pracownicy zatrudnieni - na podstawie umowy o pracę, bądź świadczący usługi na podstawie umów cywilnoprawnych (w tym także stażyści oraz praktykanci) - przy przetwarzaniu danych osobowych

zobowiązani są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 1 do niniejszej Polityki.

4. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Kodeksu Pracy.

3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych lub przez upoważnioną osobę w jego imieniu. Upoważnienia nadawane są indywidualnie, odrębnie do każdego zbioru danych osobowych, ze wskazaniem jego podzbioru przed rozpoczęciem przez pracownika przetwarzania danych osobowych w danym zbiorze.

2. Upoważnienie do przetwarzania danych osobowych mogą uzyskać wyłącznie pracownicy w tym także stażyści oraz praktykanci i, a także osoby fizyczne, współpracujące z UCZNIOWSKI KLUB SPORTOWY DĄB 19 i pozostające w jego strukturze organizacyjnej (w szczególności poprzez realizację usług w lokalizacjach Administratora Danych z wykorzystaniem stosowanych urządzeń lub systemów), które uzyskują dostęp do danych osobowych w związku ze świadczeniem na rzecz i usług na podstawie umów cywilnoprawnych.

3. Procedura zarządzania upoważnieniami do przetwarzania danych osobowych w zbiorach danych osobowych dla osób nie będących pracownikami UCZNIOWSKI KLUB SPORTOWY DĄB 19, w oparciu o zawarte pomiędzy Administratorem Danych a innym pomiotem umowy powierzenia przetwarzania danych osobowych, wskazana jest w przedmiotowych umowach o powierzeniu przetwarzania danych osobowych.

4. Upoważnienia do przetwarzania danych osobowych dla osób Zarządzających Zbiorami Danych nadawane są w imieniu Administratora Danych przez właściciela.

5. Upoważnienia dla pozostałych pracowników i, biorących udział w procesach przetwarzania danych, nadawane są przez osoby Zarządzające Zbiorami Danych. Przed nadaniem upoważnienia, w razie wątpliwości co do zakresu upoważnienia Zarządzający Zbiorem Danych występuje z wnioskiem konsultacyjnym do Administratora Danych, który podejmuje decyzję o akceptacji bądź odmowie akceptacji przyznania upoważnienia do przetwarzania danych osobowych dla pracownika. W sytuacjach niebudzących zastrzeżeń Zarządzający Zbiorem Danych podpisuje i nadaje upoważnienie. Osoba Zarządzająca Zbiorem Danych informuje osoby uczestniczące w procesie nadawania upoważnień o jego przebiegu i rezultacie.

6. Administrator Danych oraz Osoby Zarządzające Zbiorem Danych ponoszą odpowiedzialność za przyznanie (utrzymywanie) zbyt szerokich uprawnień, w stosunku do realizowanych przez pracownika zadań zwłaszcza, jeżeli w związku z tym doszło do naruszenia bezpieczeństwa przetwarzania danych osobowych oraz odpowiadają za spełnienie innych wymagań dotyczących dopuszczenia do przetwarzania danych osobowych przewidzianych w niniejszym Rozdziale.
7. Przed nadaniem upoważnienia pracownik, któremu ma być ono nadane, bierze udział w szkoleniu z zakresu przetwarzania i ochrony danych osobowych. Osobami odpowiedzialnymi za przeprowadzenie szkoleń, opracowanie ich programu i zapewnienie jego realizacji są Administrator Danych wraz z osobą przeszkoloną w zakresie RODO.

7.1. Administrator Danych przed każdym szkoleniem indywidualnie określi zakres tematyczny i główne grupy poruszanych zagadnień, w tym obejmujące podstawy prawne ochrony danych osobowych, obowiązującą w klubie dokumentację przetwarzanych danych oraz szczegółowe zasady, przetwarzania danych osobowych w poszczególnych zbiorach danych osobowych.

7.1.1. Administrator Danych zobowiązany jest:

- we własnym zakresie stale rozwijać wiedzę, umożliwiającą mu pełnienie powierzonej funkcji (w szczególności poprzez uczestnictwo w szkoleniach umożliwiających poszerzenie zakresu informacji dotyczących procesów związanych z przetwarzaniem danych osobowych),
- na bieżąco monitorować zmiany przepisów prawnych regulujących procesy przetwarzania i ochrony danych uwzględniając wszelkie zmiany

7.1.2. Zarządzający Zbiorem Danych Osobowych szkolony jest przez Administratora Danych lub inną wskazaną przez niego osobę (szkolenie wprowadzające). W ramach szkolenia jest on zapoznawany z:

- ogólnymi zagadnieniami związanymi z ochroną danych osobowych,
- szczegółowymi procedurami związanymi z ochroną danych osobowych w UCZNIOWSKI KLUB SPORTOWY DĄB 19 , a w szczególności związanymi z zarządzanymi zbiorami danych osobowych. Zarządzający Zbiorami Danych osobowych pozostaje w stałym kontakcie z Administratorem Danych i jest na bieżąco informowany o: zmianach procedur związanych z ochroną danych osobowych.
- Pracownicy, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych szkoleni są przez Administratora Danych lub inną wskazaną przez niego osobę (szkolenie wprowadzające). W ramach szkolenia są oni zapoznawani z następującymi zagadnieniami:
- podstawowymi pojęciami z zakresu ochrony danych osobowych (dane osobowe, przetwarzanie danych osobowych, dane wrażliwe, zbiór danych osobowych),
- odpowiedzialnością prawną ciążącą na osobach przetwarzających dane osobowe,
- procedurami działania w przypadku wykrycia nieuprawnionego dostępu do danych osobowych,
- sposobem postępowania w przypadku wykrycia nieprawidłowości związanych z przetwarzaniem danych osobowych.

8. W przypadku zaistnienia nadzwyczajnych okoliczności, wpływających na konieczność poszerzenia wiedzy Zarządzających Zbiorami Danych Osobowych oraz pracowników przetwarzających dane osobowe, takich jak w szczególności: gruntowna zmiana przepisów prawnych związanych z ochroną danych osobowych, Administrator Danych lub inna wskazana przez niego osoba przeprowadza szkolenie uzupełniające .

9. Szkolenie uzupełniające, zostanie przeprowadzone bez zbędnej zwłoki w odniesieniu do dnia zaistnienia nadzwyczajnych okoliczności.

10. Po odbyciu szkolenia wprowadzającego osobom biorącym udział w procesach przetwarzania danych osobowych nadawane jest upoważnienie do przetwarzania danych osobowych, wydawane jest ono w dwóch egzemplarzach, z których każdy musi być podpisany przez pracownika któremu je nadano. Jednocześnie osoba, której nadawane jest upoważnienie do przetwarzania danych osobowych zostaje

zobowiązana do stosowania obowiązujących w klubie zasad ochrony danych osobowych, poprzez złożenie własnoręcznego podpisu na wydanym jej upoważnieniu do przetwarzania danych osobowych.

- Jeden egzemplarz upoważnienia jest przechowywany jako część dokumentacji kadrowej, drugi jest wydawany pracownikowi któremu nadano upoważnienie.

- Wydanie każdego upoważnienia jest odnotowywane przez Administratora Danych w prowadzonej przez niego ewidencji upoważnień

11. Zakres nadanych pracownikowi uprawnień może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego określonych zadań w określonym czasie. W takim przypadku tryb wskazany do nadawania uprawnień określony w niniejszym Rozdziale jest właściwy również w razie aktualizacji zakresu przyznanych uprawnień dla pracownika w związku z jego dostępem do określonego zbioru danych osobowych.

12. Obligatoryjna utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:

12.1. zmiany stanowiska pracy w klubie, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,

12.2. umyślnego naruszenia zasad ochrony danych osobowych określonych w Ustawie, Rozporządzeniu, Polityce, Instrukcji,

12.3. rozwiązania stosunku pracy.

13. W przypadkach określonych w punkcie powyżej podmiot, który był właściwy do nadania upoważnienia do przetwarzania danych osobowych zobowiązany jest niezwłocznie do jego wycofania i powiadomienia Administratora Danych oraz działu kadr o konieczności dokonania zmian w prowadzonej przez nich ewidencji osób dopuszczonych do przetwarzania danych.

4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. UCZNIOWSKI KLUB SPORTOWY DĄB 19 realizując niniejszą Politykę Bezpieczeństwa, dopuszcza by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na mocy umowy powierzenia przetwarzania danych osobowych, wchodzących w skład danego zbioru danych osobowych, bądź powierzenia elementów danego zbioru w określonym celu i zakresie, podmiotowi zewnętrznemu.

2. Pisemna umowa o powierzeniu przetwarzania danych osobowych, o której mowa w niniejszym Rozdziale musi być zgodna z postanowieniami art. 31 Ustawy.

3. Powierzenia przetwarzania danych osobowych może dokonać Administrator Danych. Powierzenie przetwarzania danych osobowych może nastąpić na podstawie pisemnej umowy, aneksu do umowy lub klauzuli do umowy.

4. W przypadku, gdy powierzenie danych osobowych wynika wprost z zawartej z danym podmiotem umowy, nie ma konieczności sporządzania dodatkowo pisemnej umowy o powierzeniu przetwarzania danych osobowych.

5. Każdorazowe dokonanie powierzenia danych osobowych o którym mowa w niniejszym Rozdziale musi obligatoryjnie zostać odnotowane w wykazie zawartych umów o powierzeniu przetwarzania danych osobowych stanowiącym Załącznik nr 3 do niniejszej Polityki, prowadzonym przez Administratora Danych.

6. UCZNIOWSKI KLUB SPORTOWY DĄB 19 w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone mu przez inne podmioty. Administratorem powyższych danych są podmioty przekazujące dane osobowe w powierzenie, będące zobowiązane do zawarcia pisemnej umowy o powierzeniu przetwarzania ww. danych.

7. Dane osobowe przetwarzane w klubie mogą zostać udostępnione odbiorcom danych lub innemu podmiotowi na zasadach określonych poniżej.

8. Dane osobowe mogą być udostępniane na pisemny umotywowany wniosek osoby, której dotyczą w terminie 30 dni od daty złożenia przez nią wniosku w ramach przysługującego jej prawa do kontroli przetwarzania danych osobowych.

9. Do udostępnienia danych może dojść również w oparciu o zawartą umowę udostępnienia danych osobowych, po spełnieniu przesłanki legalności udostępnienia danych osobowych.

10. Udostępnienie danych osobowych powinno zawierać informację o tym, jakie dane osobowe zawiera zbiór, w jaki sposób zebrano dane, w jakim celu i zakresie dane są przetwarzane oraz w jakim zakresie oraz komu dane zostały udostępnione.

11. Udostępnienie danych osobowych odbiorcom danych może odbywać się w celu włączenia danych do zbioru lub w celach innych niż włączenie danych do zbioru.

12. Wnioski o udostępnienie danych, o którym mowa w Punkcie 8 przekazywane są do Administratora Danych, który je opiniuje i odnotowuje fakt udostępnienia w prowadzonej ewidencji, której wzór zawiera Załącznik nr 5. Odnotowanie faktu udostępnienia danych osobowych następuje również w sytuacji udostępnienia danych na podstawie stosownej umowy, o której mowa w pkt 9.

13. Faktycznego udostępnienia danych lub przekazania wnioskującemu informacji o nieudostępnieniu wnioskowanych danych dokonuje Zarządzający Zbiorem Danych Osobowych, odpowiedzialny za zbiór, w którym przetwarzane są dane objęte wnioskiem.

14. W przypadku konieczności ujawnienia do wiadomości publicznej danych osobowych przetwarzanych w klubie, informacje o tym przekazuje się do Administratora Danych, który dokonuje oceny legalności takiego ujawnienia.

5. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w strukturze Administratora Danych sprawuje osoba wyznaczona przez właściciela i przeszkolona, certyfikowana w zakresie Ochrony Danych Osobowych.

2. Czynności kontrolne przeprowadzane są raz w roku. Kontrolą, o której mowa w pkt 1, mogą zostać objęte stanowiska/osoby wyodrębnione w strukturze Administratora Danych w celu ustalenia, czy w ich obszarze funkcjonowania nie znajdują się dane osobowe, które powinny zostać poddane zasadom ochrony przewidzianym w Ustawie, Rozporządzeniu oraz dokumentacji przetwarzania danych.

3. Z czynności audytowych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i czynności przeprowadzonych w jej trakcie. We wnioskach protokołu dokonuje się całościowej

oceny stanu ochrony danych przetwarzanych przez Administratora Danych oraz wskazuje występujące w tym zakresie uchybienia wraz ze sposobami i terminem ich usunięcia.

4. Protokół sporządzany jest w dwóch egzemplarzach i podpisywany jest przez osoby wykonujące czynności kontrolne oraz obowiązkowo przez osobę upoważnioną do dysponowania danymi. Jednen egzemplarz protokołu pozostaje w dokumentacji Administratora a drugi otrzymuje osoba upoważniona do przetwarzania danych.

5. Osobom wymienionym w pkt 1 przysługuje prawo do wykonania czynności sprawdzających w zakresie weryfikacji usunięcia przez osobę upoważnioną uchybień i wykonania innych zaleceń wskazanych w protokole z przeprowadzonego audytu. Z czynności tych spisywany jest protokół. W przypadku nie wykonania zaleceń pokontrolnych Audytor informuje pisemnie o tym fakcie Administratora danych wnioskując o podjęcie działań dyscyplinujących.

6. SZCZEGÓŁOWY WYKAZ PRZETWARZANYCH ZBIORÓW DANYCH OSOBOWYCH

1. W klubie wyodrębnione zostały zbiory danych osobowych, których wykaz wraz ze wskazaniem programów stosowanych do ich przetwarzania oraz opisem struktury zbiorów danych osobowych wskazującym zawartość poszczególnych pól informacyjnych i powiązań między nimi zawiera Wykaz Zbiorów Danych Osobowych stanowiący Załącznik nr 4 do niniejszej Polityki.

2. Pomiędzy systemami informatycznymi służącymi do przetwarzania danych osobowych funkcjonującymi w klubie, nie występuje wzajemny przepływ danych osobowych.

7. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Wykaz budynków tworzących obszar w którym przetwarzane są dane osobowe:

1. Siedziba Uczniowskiego Klubu Sportowego Dąb 19

8. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

1. ŚRODKI TECHNICZNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

Środek techniczny	Uwagi
Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.	
Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym pokoju.	Zabezpieczenie to funkcjonuje w odniesieniu nie do każdego z wyodrębnionych zbiorów.
Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym pokoju, w zamkniętej szafie	
Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolno stojącej gaśnicy.	
Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów	

2. ŚRODKI ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

Środek organizacyjny	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych	
Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych	
Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych	
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych	
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy	

Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym oraz zabezpieczone hasłem	
Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.	

3. ZASADY PRZEGLĄDANIA I KONSERWACJI SYSTEMU

Przegląd i konserwacja zbiorów danych dokonywane są poprzez:
a) badanie spójności bazy danych,
b) uruchamianie zapytań do bazy danych w celu analizy danych,
c) przegląd wydruków po wyznaczonych procesach,
d) sprawdzanie zgodności danych z dokumentami,
e) analiza zgłaszanych uwag użytkowników.

Przeglądu i konserwacji dokonują specjalista ds Informatyki w porozumieniu z Administratorem Danych

W przypadku zlecenia wykonywania czynności, o których mowa wyżej, podmiotowi zewnętrznemu, wszelkie prace powinny odbywać się pod nadzorem Administratora Dannych.

9. ZAŁĄCZNIKI

Załącznik nr 1 – Wzór upoważnienia do przetwarzania danych osobowych
Załącznik nr 2 – Ewidencja osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 3 – Wykaz zawartych umów o powierzeniu przetwarzania danych osobowych/udostępnieniu danych osobowych.
Załącznik nr 4 – Rejestr kategorii przetwarzań danych osobowych