ZARZĄDZENIE NR 4/2019

Rektora Akademii Wychowania Fizycznego im. Bronisława Czecha w Krakowie z dnia 12 lutego 2019 roku w sprawie ochrony danych w Akademii Wychowania Fizycznego im. Bronisława Czecha w Krakowie

Na podstawie art. 23 ustawy z dnia 20 lipca 2018 roku - *Prawo o szkolnictwie wyższym i nauce* (Dz.U. z 2018 r. poz. 1668 z późn. zm.) w celu realizacji postanowień Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku *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), zwane dalej RODO, zarządzam co następuje:

§ 1

1. Wprowadzam *„Politykę Bezpieczeństwa"* stanowiącą **Załącznik nr 1** niniejszego Zarządzenia.
2. Wprowadzam *„Instrukcję zarządzania systemem informatycznym"* stanowiącą **Załącznik nr 2** niniejszego Zarządzenia.

§ 2

1. Akademia Wychowania Fizycznego im. Bronisława Czecha w Krakowie zapewnia ochronę danych osobowych na zasadach określonych postanowieniami RODO.
2. Administratorem danych osobowych, zwanym dalej „Administratorem" jest Akademia Wychowania Fizycznego im. Bronisława Czecha w Krakowie, reprezentowana przez Rektora.

§ 3

Przetwarzanie przez Administratora danych osobowych na Akademii Wychowania Fizycznego im. Bronisława Czecha w Krakowie służy realizacji zadań, obowiązków lub uprawnień wynikających z ustawy Prawo o szkolnictwie wyższym i nauce oraz Statutu Uczelni.

§ 4

1. Za obowiązki nakładane na Administratora przez RODO odpowiadają:
   1) Inspektor Ochrony Danych,
   2) Osoby upoważnione.
2. Inspektora Ochrony Danych wyznacza Rektor.
3. Inspektor Ochrony Danych podlega bezpośrednio Rektorowi.
4. Administrator niezwłocznie po wyznaczeniu Inspektora Ochrony Danych podaje jego dane na stronie internetowej Uczelni.

§ 5

1. Administrator uwzględniając charakter, zakres, cel i kontekst przetwarzania danych osobowych oraz ryzyko ich naruszenia, wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia prawidłowego i zgodnego z prawem przetwarzania danych osobowych.

2. Środki techniczne i organizacyjne, o których mowa w ust. 1 powyżej, obejmują wdrożenie odpowiednich procedur, polityk ochrony danych oraz prowadzenia odpowiednich rejestrów.

§ 6

1. Osoby, których dane są przetwarzane przez Administratora mają prawo do ochrony swoich danych osobowych, w szczególności mają prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania jak również prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych.
2. Osoby, których dane dotyczą, mają prawo żądać od Administratora niezwłocznego usunięcia dotyczących ich danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z poniższych okoliczności:
   1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
   2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
   3) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania z przyczyn związanych z jej szczególną sytuacją i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania jej danych na potrzeby marketingu bezpośredniego,
   4) dane osobowe były przetwarzane niezgodnie z prawem,
   5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator,
   6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w RODO.
3. Żądanie usunięcia przez Administratora danych osobowych, nie ma zastosowania w zakresie w jakim przetwarzanie przez Administratora danych osobowych jest niezbędne:
   1) do wywiązania się przez Administratora z ciążącego na nim prawnego obowiązku,
   2) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych,
   3) do celów ustalenia, dochodzenia roszczeń lub ochrony praw.

§ 7

Administrator może powierzyć w drodze umowy spełniającej warunki określone w RODO, innemu podmiotowi przetwarzanie danych osobowych. Podmiot ten zobowiązany jest do przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w tej umowie.

§ 8

1. Szczegółowe unormowania w zakresie zarządzania, ochrony, przetwarzania danych osobowych, a także postępowania w przypadku naruszenia zasad ochrony danych osobowych określa Polityka Bezpieczeństwa stanowiąca **Załącznik nr 1** niniejszego Zarządzenia.
2. Szczegółowe unormowania w zakresie zasad eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych określa Instrukcja zarządzania systemem informatycznym" stanowiąca **Załącznik nr 2** niniejszego Zarządzenia.

§ 9

1. Zarządzenie wchodzi w życie z dniem ogłoszenia.
2. Traci moc Zarządzenie nr 28/2008 z dnia 5 listopada 2008 roku ***w sprawie wdrożenia „Polityki Bezpieczeństwa" oraz „Instrukcji zarządzania systemem informatycznym„ w Akademii***.

REKTOR

Prof. dr hab. Aleksander Tyka

Z upoważnienia
adw. Macieja Skotnickiego

Załącznik nr 1
do Zarządzenia Rektora Nr 4/2019
z 12 lutego 2019 roku

POLITYKA BEZPIECZEŃSTWA

Akademia Wychowania Fizycznego z siedzibą w Krakowie

WSTĘP

INFORMACJE OGÓLNE

1. Polityka Bezpieczeństwa została opracowana w oparciu o wytyczne zawarte w następujących aktach prawnych:
   1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), dalej „Rozporządzenie",
   2) ustawy z dnia 10 maja 2018 r., o ochronie danych osobowych (Dz.U. z 2018 roku poz. 1000), dalej „Ustawa".
2. Określenia i skróty użyte w niniejszej Polityce Bezpieczeństwa oznaczają:
   1) **Administrator Danych – Akademia Wychowania Fizycznego im. Bronisława Czecha w Krakowie**, Al. Jana Pawła II 78, 31-571 Kraków, posiadająca numer NIP: 6750001952, REGON: 000327847, zwana dalej „Administratorem",
   2) **Inspektor lub IOD** – Inspektor Ochrony Danych,
   3) **Dane osobowe** - oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
   4) **Osoba upoważniona** – osoba posiadająca pisemne upoważnienie nadane przez Administratora Danych do przetwarzania danych osobowych, w zakresie określonym w upoważnieniu,
   5) **Pracownik** – osoba zatrudniona w Akademii Wychowania Fizycznego im. Bronisława Czecha w Krakowie na podstawie umowy o pracę, mianowania lub wykonująca usługi na podstawie umów cywilnoprawnych,
   6) **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak 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.
3. Celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Administratora z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
4. Polityka Bezpieczeństwa dotyczy wszystkich danych osobowych przetwarzanych przez Administratora, niezależnie od formy ich przetwarzania oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

PODSTAWOWE INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH

1. Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
2. Dane osobowe są przetwarzane w następujących budynkach, pomieszczeniach lub częściach pomieszczeń:
   1) Budynek Główny AWF w Krakowie cz. A – Administracja Uczelni (Dział Księgowości, Dział Płac, Sekcja Zamówień Publicznych, Dział Kadr, Dział Nauki i Wydawnictw, Dział Informatyzacji Uczelni, Centrum Edukacji Zawodowej, Kancelaria Główna i Sekretariat

Kanclerza, Dział Nauczania i Spraw Socjalno-Bytowych Studentów, Biuro Rektora, Dział Administracji, Gospodarki Materiałowej i Zaopatrzenia, Dział Technicznej Obsługi Budynków);
2) Budynek Główny AWF w Krakowie cz. B – Biblioteka Główna, Archiwum;
3) Budynek Główny AWF w Krakowie – Pawilony Naukowo – Dydaktyczne nr I – IV – Dziekanat Wydziału Wychowania Fizycznego i Sportu, Dziekanat Wydziału Rehabilitacji Ruchowej, Dziekanat Wydziału Turystyki i Rekreacji;
4) Pawilon Socjalny – Dział Organizacji Imprez;
5) Hala Gier Sportowych – Dział Eksploatacji i Obsługi Obiektów Sportowych;
6) Zespół Krytych Pływalni – Sekcja Zespołu Krytych Pływalni;
7) Domy Studenckie nr 1,2,3 – Dział Domów Studenckich;

3. Administrator przetwarza następujące kategorie danych:
1) kandydatów do pracy,
2) pracowników,
3) kandydatów na studia,
4) studentów,
5) kontrahentów.
4. Administrator przetwarza dane w następujących programach:
1) System ERP Egeria,
2) System USOS wraz z aplikacjami stowarzyszonymi,
3) Płatnik,
4) Elektroniczny System Rekrutacyjny,
5) E-szkoła,
6) ProPubliko,
7) Serwer pocztowy,
8) Klient pocztowy,
9) Strony WWW,
10) Optidata,
11) Program Akademicki,
12) System Biblioteczny.
5. Administrator prowadzi **rejestr czynności przetwarzania** zgodnie ze wzorem stanowiącym załącznik do niniejszej Polityki Bezpieczeństwa.
6. W celu zapewnienia bezpieczeństwa informacji Administrator stosuje następujące środki ochrony, szczegółowy opis środków ochrony zawiera Instrukcja zarządzania systemem informatycznym:
1) zamykane szafy oraz pomieszczenia do których klucze wydawane są osobom uprawnionym,
2) kontrola dostępu do systemów informatycznych.

OSOBY ODPOWIEDZIALNE ZA PRZETWARZANIE DANYCH

1. Osobami odpowiedzialnymi za ochronę danych osobowych są:
1) Administrator Danych,
2) Inspektor Ochrony Danych,
3) osoby związane z Administratorem Danych stosunkiem zatrudnienia wynikającym z umowy o pracę lub związane z Administratorem Danych na podstawie umów cywilnoprawnych, w zakresie przetwarzania przez nie danych, na podstawie udzielonych przez Administratora Danych upoważnień, zwane dalej „osobami upoważnionymi",
4) osoby, którym na podstawie umowy powierzenia danych powierzone zostały do przetwarzania dane osobowe.
2. **Upoważnienie do przetwarzania danych osobowych** nadaje Administrator Danych, zgodnie ze wzorem stanowiącym załącznik do niniejszej Polityki Bezpieczeństwa.
3. Administrator prowadzi **ewidencje**, zgodnie ze wzorem stanowiącym załącznik do niniejszej Polityki Bezpieczeństwa, **osób upoważnionych do przetwarzania danych**.
4. **Sposób zarządzania użytkownikami i udzielania im dostępu** określa procedura stanowiąca załącznik do niniejszej Polityki Bezpieczeństwa.

5. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, i niniejszej Polityki Bezpieczeństwa.
6. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu umów, w tym umowy o pracę.

UMOWY POWIERZENIA PRZETWARZANIA DANYCH

1. W celu powierzenia przetwarzania danych osobowych Administrator Danych jest zobowiązany zawrzeć umowę powierzenia z podmiotem, któremu będą powierzone dane. Umowa powinna zawierać wskazanie, które dane zostają powierzone oraz w jakim celu.
2. **Wzór umowy powierzenia przetwarzania danych** stanowi załącznik do niniejszej Polityki Bezpieczeństwa.
3. Administrator Danych, w ramach rejestru czynności przetwarzania danych, prowadzi wykaz podmiotów, którym powierzone zostało przetwarzanie danych.

PODSTAWOWE ZASADY DOTYCZĄCE BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

1. Za bezpieczeństwo przetwarzania danych osobowych indywidualną odpowiedzialność ponosi każda osoba upoważniona do przetwarzania danych.
2. Osoby upoważnione do przetwarzania danych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
3. Przed rozpoczęciem przetwarzania danych osobowych każda osoba powinna sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora Danych lub IOD.
4. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, każdy jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu w sposób uniemożliwiający jego odczytanie przez inne osoby.
5. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora lub hasła dostępu innej osoby.
6. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego.
7. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej osoby upoważnione zobowiązane są do stosowania zasady tzw. „czystego biurka", tj. do pozostawiania materiałów zawierających dane osobowe w miejscu uniemożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
8. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
9. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
10. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej, chyba że dane te są w odpowiedni sposób zabezpieczone przed nieuprawnionym dostępem.
11. Zakończenie pracy w systemie informatycznym powinno być poprzedzone sporządzeniem, w miarę potrzeby, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych płyt CD, pendrive i innych, zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu.

12. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.
13. W przypadku wystąpienia incydentów dotyczących bezpieczeństwa danych osobowych pracownicy zobowiązani są postępować zgodnie z **Procedurą postępowania w sytuacji incydentów ochrony danych osobowych**, która stanowi załącznik do niniejszej Polityki Bezpieczeństwa.
14. Dane osobowe są usuwane na żądanie osoby, której dane dotyczą lub w wyniku aktualizacji baz danych Administratora i ustaniu podstawy przetwarzania danych. Z usunięcia danych spisywany jest **protokół**, którego wzór stanowi załącznik do niniejszej Polityki Bezpieczeństwa. Administrator prowadzi również **rejestr usuniętych danych**, zgodnie ze wzorem stanowiącym załącznik do niniejszej Polityki Bezpieczeństwa.
15. Administrator odpowiada na żądania osób w zakresie ich danych osobowych, które to żądania zgłaszane są za pośrednictwem pisma lub drogą komunikacji elektronicznej. Administrator prowadzi rejestr żądań dotyczących danych osobowych.
16. Administrator, za pośrednictwem wyznaczonej do tego osoby, odpowiada na żądania bez zbędnej zwłoki, przy czym nie później niż w terminie 1 miesiąca od dnia otrzymania żądania. W przypadku uzasadnionych wątpliwości co do tożsamości osoby zgłaszającej żądanie Administrator może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Nadzór i kontrolę nad ochroną danych osobowych sprawuje Administrator Danych lub IOD.
2. Administrator Danych lub IOD dokonują czynności kontrolnych w ramach sprawdzeń zgodności przetwarzania danych osobowych z przepisami Rozporządzenia, Ustawy oraz niniejszej polityki bezpieczeństwa i procedurami określonymi w załącznikach do niej.
3. W toku sprawdzenia Administrator Danych lub IOD dokonują i dokumentują czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami Rozporządzenia oraz Ustawy oraz do opracowania sprawozdania.
4. Po zakończeniu sprawdzenia, Administrator Danych lub IOD przygotowują, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
5. Administrator Danych lub IOD, co do zasady, ma prawo do kontroli podmiotów, którym powierzono przetwarzanie danych osobowych, chyba, że umowa o powierzenie przetwarzania danych nie zawiera stosownych postanowień.
6. Administratora Danych lub IOD w związku z przetwarzaniem danych osobowych współpracują z organem nadzorczym, a także pełnią funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych.

REKTOR

Prof. dr hab. Aleksander Tyka

ZAŁĄCZNIKI

1) Wzór rejestru czynności przetwarzania.
2) Wzór upoważnienia do przetwarzania danych osobowych - dla pracowników zatrudnionych.
3) Wzór upoważnienia do przetwarzania danych osobowych - dla pracowników nowo przyjmowanych.
4) Wzór oświadczenia składanego po zakończeniu stosunku pracy lub cofnięciu upoważnienia.
5) Wzór ewidencji osób upoważnionych.
6) Wzór umowy powierzenia przetwarzania danych osobowych.
7) Procedura postępowania w sytuacji incydentów ochrony danych osobowych.
8) Procedura zarządzania dostępem i użytkownikami.
9) Rejestr żądań dotyczących przetwarzania danych AWF.
10) Protokół usunięcia danych - przetwarzanych elektronicznie.
11) Protokół usunięcia danych - przetwarzanych manualnie.
12) Rejestr usuniętych danych.

Załącznik nr 1 do
Polityki Bezpieczeństwa

WZÓR REJESTRU CZYNNOŚCI PRZETWARZANYCH

Lp.	Nazwa podmiotu przetwarzającego	Dane kontaktowe	Umowa powierzenia przetwarzania danych	Czynność
1.				
2.				
3.				
4.				
5.				

Lp.	Dane podmiotu przetwarzającego	Dane administratora	Kategorie przetwarzania danych	Kategorie osób	Transfer do państwa trzeciego	Ogólny opis środków technicznych i organizacyjnych
1.	Akademia Wychowania Fizycznego im. Bronisława Czecha w Krakowie, NIP: 6750001952, REGON: 000327847, Al. Jana Pawła II 78, 31-571 Kraków					
1						
2						
3						
4						

Załącznik nr 2 do
Polityki Bezpieczeństwa

Kraków, dn. _____ r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
(dla pracowników zatrudnionych)

Działając imieniem Pracodawcy, tj. **Akademii Wychowania Fizycznego im. Bronisława Czecha w Krakowie**, Al. Jana Pawła II 78, 31-571 Kraków, posiadającej numer NIP: 6750001952, REGON: 000327847, będącej administratorem danych osobowych, na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO,** niniejszym upoważniam:

_____ (*imię, nazwisko*)

_____ (*stanowisko*)

do przetwarzania danych osobowych _____,
w zakresie niezbędnym do wykonywania pełnionych obowiązków służbowych na zajmowanym stanowisku. W związku z udzielonym upoważnieniem otrzymuje Pani/Pan dostęp do danych znajdujących się w następujących programach: _____.

Upoważnienie udzielane jest na okres zatrudnienia na powyższym stanowisku, z tym, że może być w każdym czasie odwołane przez Pracodawcę, w szczególności w razie naruszenia przez Pracownika przyjętych u Pracodawcy zasad dotyczących przetwarzania danych osobowych.

_____

/podpis Pracodawcy/

Załącznik nr 3 do
Polityki Bezpieczeństwa

Kraków, dn. _____ r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
(dla pracowników nowo przyjmowanych)

Działając imieniem Pracodawcy, tj. **Akademii Wychowania Fizycznego im. Bronisława Czecha w Krakowie**, Al. Jana Pawła II 78, 31-571 Kraków, posiadającej numer NIP: 6750001952, REGON: 000327847, będącej administratorem danych osobowych, na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO,** niniejszym oświadczam, iż z dniem _____ upoważniona została:

_____ (*imię, nazwisko*)

_____ (*stanowisko*)

do przetwarzania danych osobowych _____,
w zakresie niezbędnym do wykonywania pełnionych obowiązków służbowych na zajmowanym stanowisku. W związku z udzielonym upoważnieniem otrzymała(otrzymał) Pani/Pan dostęp do danych znajdujących się w następujących programach: _____.

Upoważnienie udzielane jest na okres zatrudnienia na powyższym stanowisku, z tym, że może być w każdym czasie odwołane przez Pracodawcę, w szczególności w razie naruszenia przez Pracownika przyjętych u Pracodawcy zasad dotyczących przetwarzania danych osobowych.

_____

/podpis Pracodawcy/

Załącznik nr 4 do
Polityki Bezpieczeństwa

Kraków, dn. _____ r.

OŚWIADCZENIE PRACOWNIKA
składane po zakończeniu stosunku pracy lub cofnięciu upoważnienia

W związku z udzielonym mi przez Pracodawcę, tj. **Akademię Wychowania Fizycznego im. Bronisława Czecha w Krakowie**, Al. Jana Pawła II 78, 31-571 Kraków, posiadającą numer NIP: 6750001952, REGON: 000327847 będącą administratorem danych osobowych, upoważnieniem z dnia _____ do przetwarzania danych osobowych oświadczam, iż zapoznałam (zapoznałem) się z procedurami dotyczącymi przetwarzania danych osobowych stosowanymi u Pracodawcy.

Jednocześnie zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobu ich zabezpieczenia po zakończeniu stosunku pracy lub cofnięciu upoważnienia

_____

/podpis Pracownika/

Załącznik nr 5 do
Polityki Bezpieczeństwa

WZÓR EWIDENCJI OSÓB UPOWAŻNIONYCH

Upoważnienia do przetwarzania danych osobowych

Lp.	Imię i nazwisko osoby upoważnionej	Data upoważnienia	Stanowisko	Zakres upoważnienia	Programy, do których udzielono dostępu	Czas obowiązywania upoważnienia	Oświadczenia upoważnionego o zapoznaniu się z procedurami przetwarzania danych	Data nadania dostępu do danych i bazy danych	Data i podstawa ograniczenia dostępu do danych	Data i podstawa odebrania dostępu do danych
				Niezbędny do wykonania obowiązków pracowniczych		Na czas zatrudnienia				

Umowa o powierzanie przetwarzania danych osobowych

zawarta w dniu _____, pomiędzy

Akademią Wychowania Fizycznego im. Bronisława Czecha w Krakowie, Al. Jana Pawła II 78, 31-571 Kraków, posiadającą numer NIP: 6750001952, REGON: 000327847, reprezentowana przez Rektora _____, zwaną dalej „Administratorem Danych" lub „Stroną"

a

_____ zwaną dalej „Przetwarzającym Dane" lub „Stroną",

oba podmioty zwane dalej łącznie „Stronami",

zawarta na podstawie art. 28 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej: RODO

[Przedmiot umowy]

§ 1

1. W związku z zwartą między Stronami umową dotyczącą _____, zwaną dalej „Umową podstawową", konieczne jest powierzenie przez Administratora przetwarzania danych Przetwarzającemu Dane.
2. Przedmiotem niniejszej umowy jest powierzenie przez Administratora Danych do przetwarzania przez Przetwarzającego Dane, danych osobowych – zwanych dalej „danymi osobowymi" – _____[określenie kategorii osób, których dane dotyczą], w zakresie _____[określenie celu przekazania], w tym obejmującym przede wszystkim następujące dane osobowe:
   1) imię i nazwisko,
   2) adres,
   3) adres e-mail,
   4) numer telefonu.
3. Przetwarzający Dane zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Przetwarzający Dane oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.

[Sposób przetwarzania przekazanych danych osobowych]

§ 2

1. Dane osobowe będą przetwarzane przez Przetwarzającego Dane w ten sposób, że _____
_____.
2. Dane osobowe będą przetwarzane przy użyciu udostępnionych przez Przetwarzającego Dane aplikacji umożliwiających przetwarzanie danych osobowych za pomocą zewnętrznego oprogramowania i infrastruktury nienależących do Administratora Danych lub formularzy papierowych.

[Obowiązki podmiotu przetwarzającego]

§ 3

1. Przetwarzający Dane 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 RODO.
2. Przetwarzający Dane zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Przetwarzający Dane zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Przetwarzający Dane zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b RODO) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich u Przetwarzającego Dane, jak i po jego ustaniu.
5. Przetwarzający Dane po zakończeniu świadczenia usług związanych z przetwarzaniem zwraca Administratorowi Danych 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 Przetwarzający Dane pomaga Administratorowi Danych w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
7. Przetwarzający Dane po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi Danych w ciągu 24h.

[Prawo kontroli]

§4

1. Administrator Danych zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo kontroli, czy środki zastosowane przez Przetwarzającego Dane przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator Danych realizować będzie prawo kontroli w godzinach pracy Przetwarzającego Dane i z co najmniej 7 (siedmio) dniowym jego uprzedzeniem.
3. Przetwarzający Dane zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora Danych nie dłuższym niż 7 dni.
4. Przetwarzający Dane udostępnia Administratorowi Danych wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

[Dalsze powierzenie danych do przetwarzania]

§5

1. Przetwarzający Dane, bez uprzedniej zgody Administratora Danych, nie może powierzyć danych osobowych objętych niniejszą umową do dalszego przetwarzania podwykonawcom.
2. Przetwarzający Dane ponosi pełną odpowiedzialność wobec Administratora Danych za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

[Odpowiedzialność Podmiotu przetwarzającego]

§ 6

1. Przetwarzający Dane 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. Przetwarzający Dane zobowiązuje się do niezwłocznego poinformowania Administratora Danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez niego danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Przetwarzającego Dane, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Przetwarzającego Dane tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez właściwe organy administracyjne. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora Danych.

[Czas obowiązywania umowy]

§7

1. Niniejsza umowa zostaje zawarta na czas obowiązywania Umowy podstawowej.
2. Administrator Danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Przetwarzający Dane:
   1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   2) przetwarza dane osobowe w sposób niezgodny z umową;
   3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora Danych.

[Zasady zachowania poufności]

§8

1. Przetwarzający Dane 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. Przetwarzający Dane 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 niniejszej umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

[Postanowienia końcowe]

§9

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.
2. W sprawach nieuregulowanych zastosowanie będą miały prawa polskiego oraz właściwe przepisy prawa europejskiego, w tym RODO.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla siedziby Administratora Danych.

Administrator Danych	Przetwarzający Dane

PROCEDURA POSTĘPOWANIA W SYTUACJI INCYDENTÓW OCHRONY DANYCH OSOBOWYCH

§ 1

1. Administratorem danych jest **Akademia Wychowania Fizycznego im. Bronisława Czecha w Krakowie, Al. Jana Pawła II 78, 31-571 Kraków, posiadająca numer NIP: 6750001952, REGON: 000327847**, zwana dalej „Administratorem".
2. Administrator wyznaczy osobę upoważnioną do koordynacji procedur związanych z przetwarzaniem danych osobowych (dalej „osoba upoważniona") lub Inspektora ochrony danych (dalej „IOD").
3. Celem niniejszej procedury jest określenie zadań pracowników w zakresie:
   1) ochrony danych osobowych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą oraz ochroną zasobów technicznych;
   2) prawidłowego reagowania pracowników przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia ochrony danych osobowych lub zabezpieczeń systemu informatycznego;
   3) ograniczenia ryzyka powstania zagrożeń oraz minimalizacji skutków wystąpienia zagrożeń.

§ 2

Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie:
1) zgłoszenia osoby, której dane dotyczą lub osoby trzeciej,
2) stwierdzenia naruszenia urządzeń technicznych lub nieprawidłowości działania programów lub jakości komunikacji w sieci teleinformatycznej;
3) stwierdzenia nieprawidłowości w zawartości zbiorów danych osobowych;
4) stwierdzenia nieprawidłowości w procedurach organizacyjnych w zakładzie pracy, w tym obiegu dokumentów.

§ 3

1. Każdy pracownik Administratora w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest bezzwłocznie powiadomić bezpośredniego przełożonego lub osobę upoważnioną lub IOD.
2. Przełożony pracownika, który stwierdził zaistnienie incydentu zobowiązany jest niezwłocznie poinformować osobę upoważnioną lub IOD o zaistnieniu incydentu, chyba, że pracownik zgłosił go bezpośrednio osobie upoważnionej lub IOD.
3. Osoba upoważniona lub IOD jest zobowiązana do niezwłocznego poinformowania Administratora o zaistniałym incydencie i podjętych działaniach związanych z incydentem.
4. Do typowych zagrożeń bezpieczeństwa danych osobowych należą w szczególności:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń lub dokumentów;
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych;
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
5. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
   1) zdarzenia losowe zewnętrzne spowodowane siłą wyższą (np. pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata lub zagubienie danych);

3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów lub danych, działanie wirusów i innego szkodliwego oprogramowania).

6. W przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych osoba upoważniona lub IOD prowadzi postępowanie wyjaśniające, w toku którego:
   1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
   2) inicjuje ewentualne działania dyscyplinarne;
   3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
   4) dokumentuje czynności podjęte w prowadzonym postępowaniu poprzez sporządzenie pisemnego raportu z zagrożenia bezpieczeństwa danych osobowych, zgodnego ze wzorem stanowiącym załącznik do niniejszej procedury,
   5) podejmuje działania zapobiegawcze.
7. Osoba upoważniona lub IOD odnotowuje wystąpienia incydentu i podjęte działania w **raportach** stanowiących załącznik do niniejszej procedury.
8. Osoba upoważniona lub IOD ewidencjonuje incydent w **rejestrze incydentów**, którego wzór stanowi załącznik do Polityki bezpieczeństwa.

§ 4

1. Osoba upoważniona lub IOD jest odpowiedzialna za podjęcie działań mających zapobiec zaistnieniu identycznych lub podobnych incydentów w przyszłości. W tym celu osoba upoważniona lub IOD podejmuje właściwe działania w związku z zaistniałym incydentem, w tym:
   1) działania korygujące, które polegają na przeprowadzeniu czynności mających na celu wyeliminowanie przyczyn incydentu,
   2) działania zapobiegawcze, które polegają na wyeliminowaniu przyczyn zagrożenia lub innej potencjalnej sytuacji niepożądanej,
   3) działania kontrolne, polegające na systematycznej, niezależnej i udokumentowanej ocenie skuteczności systemu i procedur ochrony danych osobowych na podstawie wdrożonych w zakładzie pracy polityk bezpieczeństwa i instrukcji zarządzania systemu informatycznym oraz procedur związanych z dostępem do danych osobowych.

Załącznik do procedury

RAPORT Z INCYDENTU NR _____ (numer/miesiąc/rok)

Dane osoby sporządzającej raport:

Imię i nazwisko:
Stanowisko (funkcja):

Miejsce i czas zaistnienia incydentu:

Osoba lub zdarzenie powodująca incydent:

Osoba uczestnicząca w incydencie:

Opis wydarzenia związanego z incydentem:

Czy istnieje ryzyko naruszenia praw i wolności osób, których dane dotyczą (jeśli tak to w jakim stopniu: pomijalne, niskie, wysokie, maksymalne):

Opis możliwego naruszenia praw i wolności:

_____

/data i podpis/

Załącznik do procedury

RAPORT Z DZIAŁAŃ PODJĘTYCH W ZWIĄZKU Z INCYDENTEM NR _____

Dane osoby sporządzającej raport:

Imię i nazwisko:
Stanowisko (funkcja):

Oznaczenie incydentu:

Opis podjętych działań:

Prognozowany rezultat podjętych działań:

Czy poinformowano UODO?:

_____

/data i podpis/

Załącznik nr 8 do
Polityki Bezpieczeństwa

PROCEDURA ZARZĄDZANIA DOSTĘPEM I UŻYTKOWNIKAMI

§ 1

1. Administratorem danych jest **Akademia Wychowania Fizycznego im. Bronisława Czecha w Krakowie,** Al. Jana Pawła II 78, 31-571 Kraków, posiadająca numer NIP: 6750001952, REGON: 000327847, zwana dalej „Administratorem".
2. Administrator danych wyznaczy inną osobę upoważnioną do koordynacji procedur związanych z przetwarzaniem danych osobowych (dalej „osoba upoważniona") lub Inspektora ochrony danych (dalej „IOD").
3. Celem niniejszej procedury jest określenie sposobu zarządzania dostępem do danych osobowych i użytkownikami.

§ 2

1. Co do zasady, pracownik działu IT zatrudniony u Administratora (dalej „Administrator aplikacji"), nadaje każdemu z pracowników dostęp do danych osobowych przetwarzanych przez Administratora, zgodnie z pisemnym upoważnieniem
2. Na polecenie osoby upoważnionej lub IOD lub Administratora, Informatyk ogranicza lub odbiera dostęp poszczególnym osobom.
3. Administrator aplikacji nie jest uprawniony do podejmowała samodzielnych decyzji w zakresie nadawania, ograniczania lub odbierania dostępów do danych osobowych poszczególnym pracownikom.

§3

1. Osoba upoważniona otrzymuje identyfikator użytkownika i hasło.
2. Hasło stanowi wygenerowany losowo ciąg znaków. Osoba uzyskująca dostęp musi zmienić hasło przy pierwszym logowaniu do danego systemu informatycznego na hasło zgodne z zasadami tworzenia haseł.
3. Zasady tworzenia haseł w systemach, w których jest to technicznie możliwe, są następujące:
   1) hasło nie może składać się z żadnej z danych osobowych takich jak imię, nazwisko, adres, lub ich fragmentów,
   2) hasło musi składać się co najmniej z 11 znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne,
   3) hasło nie może składać się z identycznych znaków lub ciągów znaków z klawiatury,
   4) hasło nie może być jednakowe z identyfikatorem użytkownika,
   5) hasło musi być unikalne, tj. takie które nie było poprzednio stosowane przez osobę upoważnioną.
4. Osoba uzyskująca dostęp jest zobowiązana do utrzymania hasła w tajemnicy.
5. W przypadku złamania poufności hasła, osoba uzyskująca dostęp zobowiązana jest niezwłocznie:
   1) w systemach, w których jest to technicznie możliwe - samodzielnie zmienić hasło i poinformować Administratora aplikacji, przełożonego oraz IOD o złamaniu poufności hasła i dokonanej zmianie,
   2) w systemach, w których zmiana hasła musi zostać zainicjowana lub przeprowadzona przez Administratora aplikacji lub osobę posiadającą dostęp administracyjny do systemu – poinformować właściwą osobę.

Załącznik nr 9 do
Polityki Bezpieczeństwa

Rejestr żądań dotyczących przetwarzania danych AWF

LP.	Data wpływu żądania	Nadawca żądania	Sposób złożenia żądania (pocztą, elektronicznie)	Osoba, której dane dotyczą	Treść żądania	Prośba o dodatkowe informacje	Sposób realizacji żądania	Data realizacji żądania	Odmowa realizacji żądania	Przyczyny odmowy realizacji żądania	Uwagi
1.											
2.											
3.											
4.											

Załącznik nr 10 do
Polityki Bezpieczeństwa

PROTOKÓŁ USUNIĘCIA DANYCH OSOBOWYCH
(przetwarzanych elektronicznie)

Niniejszym oświadczamy, że w dniu [•] zostały usunięte dane osobowe [•], otrzymane drogą e-mailową na adres [•], w okresie od [•] do [•].

Administratorem usuniętych danych osobowych była Akademia Wychowania Fizycznego im. Bronisława Czecha w Krakowie, Al. Jana Pawła II 78, 31-571 Kraków, posiadająca numer NIP: 6750001952, REGON: 000327847.

Dane osobowe zostały usunięte w związku z [•].

Dane zostały usunięte poprzez ich wykasowanie ze skrzynek e-mailowych oraz kopii zapasowych.

W czynności usuwania przedmiotowych danych brały udział następujące osoby:

1. [•],
2. [•].

.....
(miejscowość)

.....
(dzień, miesiąc, rok)

1. _____
(podpis)

2. _____
(podpis)

Załącznik nr 11 do
Polityki Bezpieczeństwa

PROTOKÓŁ USUNIĘCIA DANYCH OSOBOWYCH
(przetwarzanych manualnie)

Niniejszym oświadczamy, że w dniu [•] zostały usunięte dane [•], a które to dane przechowywane były w [•].

Administratorem usuniętych danych osobowych była Akademia Wychowania Fizycznego im. Bronisława Czecha w Krakowie, posiadająca numer NIP: 6750001952, REGON: 000327847.

Dane osobowe zostały usunięte w związku z [•].

Dane zostały usunięte poprzez zniszczenie dokumentów w niszczarce typu [•].

W czynności usuwania przedmiotowych danych brały udział następujące osoby:

1. [•],
2. [•].

.....
(miejscowość)

.....
(dzień, miesiąc, rok)

1 _____
(podpis)

2. _____
(podpis)

Załącznik nr 12
do Polityki Bezpieczeństwa

REJESTR USUNIĘTYCH DANYCH

LP.	Oznaczenie usuniętych danych (np. kategoria danych)	Przyczyny usunięcia	Sposób usunięcia	Data usunięcia	Protokół usunięcia danych
1.					
2.					
3.					
4.					
5.					

Załącznik nr 2
do Zarządzenia Rektora Nr 4/2019
z 12 lutego 2019 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH w AKADEMII WYCHOWANIA FIZYCZNEGO IM. BRONISŁAWA CZECHA W KRAKOWIE

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Upoważnienia do przetwarzania danych osobowych nadawane są zgodnie z Polityką Bezpieczeństwa.
2. Ewidencja upoważnień do przetwarzania danych osobowych prowadzona jest zgodnie z Polityką Bezpieczeństwa i załącznikami do niej.
3. Sposób zarządzania użytkownikami, w tym sposób nadawania dostępu do danych, określa procedura stanowiąca załącznik do Polityki Bezpieczeństwa.

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu.
2. Identyfikator użytkownika i hasło tworzone są przez Administratora aplikacji zgodnie z Procedurą zarządzania dostępem i użytkownikami stanowiącą załącznik do Polityki Bezpieczeństwa.
3. Administrator aplikacji przekazuje osobie upoważnionej identyfikator użytkownika i hasło w formie dokumentu papierowego lub elektronicznego. Użytkownicy zobowiązani są do posługiwania się hasłami zgodnie z zasadami opisanymi w Polityce Bezpieczeństwa oraz Procedurze zarządzania dostępem i użytkownikami stanowiącej jej załącznik.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych

1. Użytkownicy powinni korzystać z systemów, w których przetwarzane są dane zgodnie z Polityką Bezpieczeństwa i określonymi tam podstawowymi zasadami dotyczącymi bezpieczeństwa przetwarzania danych osobowych, w tym w szczególności:
   1) Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora danych, zgodnie z Procedurą postępowania w sytuacji incydentów ochrony danych osobowych.
   2) Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu w sposób uniemożliwiający jego odczytanie przez inne osoby.
   3) Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
   4) W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.
   5) Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następuje poprzez wylogowanie się z tego systemu.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Za sporządzanie kopii zapasowych zbiorów danych przechowywanych na serwerach odpowiedzialny jest Administrator aplikacji systemu informatycznego służącego do

przetwarzania danych osobowych.

2. Za sporządzanie kopii zapasowych zbiorów danych przechowywanych na stacjach roboczych odpowiedzialny jest Użytkownik systemu informatycznego służącego do przetwarzania danych osobowych.
3. Kopie zapasowe kluczowych zbiorów danych tworzone są za pomocą oprogramowania dedykowanego lub w postaci pełnej kopii
4. Kopie zapasowe przetwarzanych danych i oprogramowania przechowywane są na wydzielonej fizycznej maszynie.
5. Kopie zapasowe powinny być kontrolowane przez Administratora danych, w szczególności pod kątem prawidłowości ich wykonania poprzez okresowe częściowe lub całkowite ich odtworzenie.
6. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
7. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.
2. W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.
3. Usuwanie danych osobowych powinno następować po konsultacji z Administratorem i z czynności tej powinien być sporządzany protokół.
4. Użytkownicy nie są uprawnieni do samodzielnego usuwania danych osobowych.

Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

1. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do sieci lokalnej w której znajduje się system informatyczny służący do przetwarzania danych osobowych stosowane są zabezpieczenia w postaci zapory sieciowej.
2. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do stanowiska komputerowego posiadającego dostęp do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest zabezpieczenie w postaci oprogramowania antywirusowego
3. Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym.
4. Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowanie oprogramowanie antywirusowe. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji

służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności Administratora danych.

2. Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.

Pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych

1. W celu zabezpieczenia fizycznego dostępu do serwerów, macierzy dyskowych i innych kluczowych urządzeń informatycznych umiejscowiono je w serwerowni.
2. W celu zabezpieczenia przed awarią zasilania kluczowych urządzeń informatycznych znajdujących się w serwerowni zastosowano zasilacze awaryjne (UPS) i zewnętrzny generator spalinowy.
3. Administrator danych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.
4. Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

Rektor

Prof. dr hab. Aleksander Tyka