Załącznik nr 1
do Uchwały nr 6/2018
Zarządu Stowarzyszenia
Uniwersytet Trzeciego Wieku
w Chrzanowie
z dnia 15 listopada 2018r.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych

w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie

Chrzanów, listopad 2018

Spis treści

CZĘŚĆ I

Dokumentacja sposobu przetwarzania danych

Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1) „**Polityce bezpieczeństwa**”, „**dokumencie**” („**PB**”) – należy przez to rozumieć „Politykę bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie”.

2) **SUTW** – należy przez to rozumieć Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie.

3) **UTW** – należy przez to rozumieć Uniwersytet Trzeciego Wieku w Chrzanowie

4) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

4a) **Osobie możliwej do zidentyfikowania** – należy przez to rozumieć osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

5) **Zbiorze danych** – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

6) **Administratorze Danych** („**AD**”) – należy przez to rozumieć Zarząd Stowarzyszenia Uniwersytet Trzeciego Wieku w Chrzanowie, reprezentowany przez Prezesa Zarządu, posiadającego zakres uprawnień w rozumieniu ustawy o ochronie danych osobowych.

7) **Administratorze Bezpieczeństwa Informacji** („**ABI**”), tj. osobie wyznaczonej do nadzorowania przestrzegania zasad ochrony danych osobowych. W SUTW nie powołuje się ABI.

8) **Osobie upoważnionej** – należy przez to rozumieć: pracownika lub członka Stowarzyszenia Uniwersytet Trzeciego Wieku w Chrzanowie, posiadającego pisemne upoważnienie do przetwarzania danych osobowych nadane przez AD.

9) **Przetwarzaniu danych** – należy przez to rozumieć 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.

9a) **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

9b) **Zabezpieczeniu danych w systemie informatycznym** – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

10) **Usuwaniu danych** – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

11) **Zgodzie osoby, której dane dotyczą** – należy przez to rozumieć oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli innej treści.

12) **Odbiorcy danych** – należy przez to rozumieć każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

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

Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie – zwanym dalej SUTW.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę SUTW.

Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie" – zwany dalej: „Polityką bezpieczeństwa", „Dokumentem", „PB", wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczony dla osób pracujących przy przetwarzaniu danych osobowych w SUTW.

Potrzeba opracowania „Polityki bezpieczeństwa" wynika z przepisów § 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Zgodnie z ww. Rozporządzeniem, Polityka Bezpieczeństwa zawiera w szczególności:

a) wykaz obiektów, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (Załącznik nr 2 do Polityki Bezpieczeństwa);

b) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami (Załącznik nr 5 do Polityki Bezpieczeństwa);

c) określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie realizując strategię bezpieczeństwa danych utrzymuje zabezpieczenia odpowiednie dla zapewnienia bezpieczeństwa informacji własnych jak i powierzonych przez członków SUTW, słuchaczy UTW i pracowników SUTW, poprzez:

- przydzielanie dostępu do informacji tylko osobom upoważnionym,
- podnoszenie świadomości użytkowników w zakresie bezpiecznego korzystania z zasobów informatycznych,
- zapewnienie zgodności działania z wymaganiami prawnymi, regulacjami wewnętrznymi oraz zapisami umownymi.

Postanowienia wynikające z polityki oraz dokumentacji systemu zarządzania bezpieczeństwem informacji są znane i respektowane przez pracowników SUTW, a także członków Zarządu SUTW.

Zarząd Stowarzyszenia Uniwersytet Trzeciego Wieku w Chrzanowie, nadzorując realizację postanowień wynikających z polityki bezpieczeństwa, zobowiązuje się do spełnienia wymagań i podejmowania wszelkich niezbędnych działań wynikających z ich naruszenia, a tym samym do ciągłego doskonalenia skuteczności Systemu Zarządzania Bezpieczeństwem Informacji.

Przepisy ogólne

Przetwarzanie danych osobowych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie dopuszczalne jest wyłącznie na zasadach określonych ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014, poz. 1182 z późn. zm.) oraz Rozporządzeniem 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. 2004, Nr 100, poz. 1024).

1. Zarządzanie przetwarzaniem danych osobowych.

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:

1) stan urządzenia, zawartość rejestru danego zbioru danych osobowych, ujawnione metody pracy mogą wskazywać na naruszenie zabezpieczeń tych danych;
2) stwierdzono naruszenie bezpieczeństwa przetwarzanych danych w rejestrze danego zbioru danych.

2. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa w danym rejestrze zbioru danych SUTW.

3. Zarząd Stowarzyszenia Uniwersytet Trzeciego Wieku w Chrzanowie Uchwałą Nr 6/2018 Zarządu SUTW z dnia 15 listopada 2018r. w sprawie ustalenia polityki bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie podjął decyzję o niepowoływaniu Administratora Bezpieczeństwa Danych; funkcje AD wypełnia Zarząd SUTW.

4.1. Administrator Danych wydaje upoważnienia do przetwarzania zbiorów danych osobowych zaewidencjonowanych w „Rejestrze zbiorów danych osobowych przetwarzanych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie".

4.2. Upoważnienie, o którym mowa w pkt. 4.1 ma formę pisemną (załącznik nr 1 „A" do „Polityki bezpieczeństwa").

4.3. Administrator Danych może w każdym czasie odwołać upoważnienie do przetwarzania danych osobowych udzielone zgodnie z pkt. 4.2.

4.4. Odwołanie upoważnienia, o którym mowa w pkt. 4.3 ma formę pisemną (załącznik nr 2 do „Polityki bezpieczeństwa").

4.5. Administrator Danych udzielania upoważnień do przetwarzania danych osobowych:

- ✓ osobom wchodzącym w skład organów statutowych SUTW,
- ✓ pracownikom Stowarzyszenia Uniwersytet Trzeciego Wieku w Chrzanowie w związku z realizacją projektu/zadania, w którym SUTW jest lub może być partnerem [niezależnie od tego, czy lider projektu/zadania (realizator) udzielił lub udzieli takiego upoważnienia, czy też nie],
- ✓ pracownikom lub współpracownikom instytucji, którym Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie powierzy – na mocy stosownej pisemnej umowy –

prowadzenie zadań z zakresu monitoringu i ewaluacji projektu/zadania, którego SUTW jest realizatorem,

- ✓ pracownikom Stowarzyszenia Uniwersytet Trzeciego Wieku w Chrzanowie w związku z pozostałymi przypadkami przetwarzania danych osobowych w SUTW.

4.6. Upoważnienia o których mowa w pkt. 4.5 mają formę pisemną (odpowiednio załącznik nr 1 „A" do „Polityki bezpieczeństwa").

4.7. Administrator Danych może w każdym czasie odwołać upoważnienie do przetwarzania danych osobowych udzielone osobom wymienionym w pkt. 4.5.

4.8. Odwołanie upoważnień, o których mowa w pkt. 4.7 ma formę pisemną (załącznik nr 2 do „Polityki bezpieczeństwa").

2. Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie, reprezentowane przez Prezesa Zarządu, jest Administratorem Danych Osobowych w rozumieniu przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i posiada zakres uprawnień w rozumieniu ww. ustawy.

3. Do zadań Administrator Danych Osobowych należy zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności poprzez:

- ochronę i bezpieczeństwo danych osobowych zawartych w zbiorach danych Stowarzyszenia Uniwersytet Trzeciego Wieku w Chrzanowie,
- sprawowania kontroli nad wprowadzaniem i udostępnianiem danych osobowych,
- sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- podejmowanie stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym lub każdym innym,
- opracowanie i aktualizowanie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, oraz przestrzegania zasad w niej określonych,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych oraz przygotowywanie upoważnień do przetwarzania danych osobowych,
- prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych,
- nadzór i kontrolę systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

2. Zakres przetwarzania danych osobowych.

1. Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie do:

1) danych osobowych przetwarzanych w systemach informatycznych oraz w tradycyjnej - papierowej formie oraz przechowywanych na wszelkich nośnikach magnetycznych, optycznych, elektronicznych takich jak: dysk twardy, dyskietka, CD/DVD, pamięć masowa typu USB-flash, a także w księgach, kwitariuszach 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.

3. Ogólne zasady przetwarzania danych osobowych.

Dane osobowe **członków SUTW** są przetwarzane w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie w następujących celach: zapewnienie właściwej organizacji pracy Stowarzyszenia, realizacja obowiązków prawnych np. zwoływanie zebrań Stowarzyszenia, udzielanie informacji, marketing działań własnych, ewidencja i zestawienia statystyczne.

Dane osobowe **słuchaczy UTW** są przetwarzane w celach: zapewnienie poprawnej jakości procesu nauczania, właściwa organizacja zajęć w ramach wykładów i warsztatów zajęciowych, wycieczek wypoczynkowo-turystycznych i wyjazdów sportowych, realizacja obowiązków prawnych np. wystawiania legitymacji słuchacza, indeksów, rozliczenia realizacji projektów grantowych, udzielanie informacji, marketing działań własnych, ewidencja i zestawienia statystyczne.

Dane osobowe **pracowników SUTW** są przetwarzane w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie w następujących celach: zapewnienie właściwej obsługi pracowniczej, realizacji obowiązków prawnych np. wynagrodzenia za pracę na rzecz SUTW i UTW, rozliczeń podatkowych, informacyjnych dla potrzeb ZUS, ustalania zakresu obowiązków itp., udzielania informacji, a także marketingu własnych działań, prowadzenia ewidencji i zestawień statystycznych.

Pod pojęciem własnych działań marketingowych należy rozumieć również okolicznościowe wydawnictwa i obecność SUTW i UTW w Internecie.

Zakres przetwarzanych danych:

a) członkowie SUTW - w formie papierowej Deklaracja Członka Stowarzyszenia, ewidencja opłacania składki członkowskiej.
   Dane będą wykorzystywane przez okres niezbędny do realizacji opisanych powyżej celów, jednak nie dłużej niż rok od chwili ustania członkostwa w SUTW, chyba że wcześniej zostanie wycofana zgoda na przetwarzanie danych, zawartych w Deklaracji Członka Stowarzyszenia.
b) słuchacze UTW - w formie papierowej Karta zgłoszenia słuchacza, Księga słuchaczy UTW, w formie elektronicznej dane osobowe zawarte w Karcie zgłoszenia słuchacza oraz Księga słuchaczy.
   Dane będą wykorzystywane przez okres niezbędny do realizacji opisanych powyżej celów, jednak nie dłużej niż rok od chwili zaprzestania uczestniczenia w zajęciach UTW i wniesienia ostatniej opłaty za semestr, chyba że wcześniej zostanie wycofana zgoda na przetwarzanie danych, zawartych w Karcie zgłoszenia słuchacza.
c) pracownicy SUTW – w formie papierowej i/lub elektronicznej w zakresie niezbędnym dla celów rozliczeniowych.
   Dane będą wykorzystywane przez okres niezbędny do realizacji opisanych powyżej celów, zgodnie z obowiązującymi przepisami dotyczącymi wynagrodzeń pracowniczych.

Ochrona danych osobowych:

Każdy słuchacz UTW i członek SUTW może złożyć do SUTW wniosek o dostęp do swoich danych osobowych (o informację o przetwarzanych danych osobowych oraz kopię danych), sprostowanie danych, gdy są one nieprawidłowe, usunięcie lub ograniczenie przetwarzania danych osobowych.

Ma również prawo wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych, jeżeli uważa, że przetwarzanie jego danych osobowych narusza przepisy prawa.

Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie nie zamierza posiadanych danych osobowych swoich członków i słuchaczy przekazywać innym podmiotom – oprócz ich wykorzystania w celu dokonania ubezpieczeń niezbędnych przy organizowaniu wyjazdów grupowych, w tym współorganizowanych przez UTW.

Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie nie zamierza posiadanych danych osobowych swoich pracowników przekazywać innym podmiotom – oprócz ich wykorzystania w celu dokonania niezbędnych rozliczeń finansowych, w tym ubezpieczeń społecznych i rozliczeń fiskalnych.

Każdy słuchacz UTW i członek SUTW oraz pracownik SUTW po zapoznaniu się z Klauzulą informacyjną RODO wyraża w formie pisemnej zgodę na przetwarzanie danych osobowych, zgodnie z Załącznikami nr 3 lub nr 4, ewentualnie 8 „A" do niniejszej Polityki bezpieczeństwa.

Rozdział 1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w SUTW

Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie zajmuje się prowadzeniem placówki edukacyjnej dla seniorów pod nazwą Uniwersytet Trzeciego Wieku w Chrzanowie. Zgodnie ze Statutem SUTW celem Stowarzyszenia jest prowadzenie edukacji w różnych dziedzinach nauk, w tym medycyny i profilaktyki zdrowia; aktywizacja społeczna osób starszych poprzez uczestnictwo w różnych formach życia społecznego; propagowanie i popieranie różnorodnych form aktywności intelektualnej, psychicznej i fizycznej; promowanie aktywnych form spędzania wolnego czasu i zdrowego stylu życia; podejmowanie działań zmierzających do utrzymania i zacieśniania więzi i kontaktów osobistych między mieszkańcami powiatu, a szczególnie pomiędzy osobami starszymi i młodym pokoleniem; upowszechnianie wiedzy o ziemi chrzanowskiej, poprzez prezentowanie dorobku kulturalno-społecznego miasta i regionu, ciekawych tras turystycznych oraz organizowanie spotkań ze znanymi osobami zasłużonymi dla kultury i turystyki regionu i Polski; prowadzenie działalności w zakresie walki z wszelkiego rodzaju uzależnieniami; prowadzenie działalności na rzecz osób niepełnosprawnych.

Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie realizuje swoje cele w szczególności poprzez prowadzenie działalności edukacyjno-informacyjnej, a zwłaszcza poprzez organizację wykładów, seminariów, lektoratów języków obcych, warsztatów, spotkań integracyjnych, prelekcji, wystaw, koncertów i innych zajęć; prowadzenie praktycznych zajęć z zakresu gimnastyki relaksacyjnej i rekreacji, organizowanie wycieczek turystycznych i krajoznawczych (krajowych i zagranicznych); współpracę z krajowymi i zagranicznymi uniwersytetami trzeciego wieku; współpracę ze szkołami wyższymi, placówkami naukowo-badawczymi, instytucjami rządowymi, jednostkami samorządu terytorialnego oraz instytucjami samorządowymi, organizacjami pozarządowymi oraz środkami masowego przekazu, a także z osobami o uznanym autorytecie; prowadzenie działalności wydawniczej oraz strony internetowej Stowarzyszenia; prowadzenie działalności w zakresie porad obywatelskich; występowanie z wnioskami i opiniami do właściwych władz, urzędów, instytucji, organizacji i fundacji w sprawach związanych z działalnością Stowarzyszenia oraz inne działania sprzyjające rozwojowi i realizacji celów statutowych.

SUTW do realizacji swoich celów zatrudnia pracowników (sekretariat, księgowość, wykładowcy, instruktorzy) na zasadach umowy zlecenia lub umowy o dzieło. Rachunkowość prowadzona jest zgodnie z obowiązującymi w tym zakresie przepisami prawa – Statut SUTW §31 p.4.

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

Siedziba organizacji znajduje się przy **ul. Focha 3 w Chrzanowie** w wolnostojącym budynku, będącym siedzibą **Powiatowego Centrum Kształcenia Ustawicznego** (PCKU). Właścicielem obiektu jest Starostwo Powiatowe, jest to budynek wielokondygnacyjny, w którym SUTW wynajmuje dwa pomieszczenia (SEKRETARIAT I BIURO PREZESA) z jednym wejściem, zlokalizowane na wysokim parterze.

Do lokalu SUTW (SEKRETARIATU) prowadzą z korytarza głównego drzwi drewniane, z jednym zamkiem. Z pomieszczenia SEKRETARIATU do pomieszczenia BIURA PREZESA prowadzą drzwi drewniane z jednym zamkiem. Drzwi nie są plombowane, okna nie są okratowane.

W SEKRETARIACIE zlokalizowany jest system komputerowy składający się z laptopa oraz drukarki wielofunkcyjnej. Laptop wykorzystywany jest m.in. do gromadzenia i przetwarzania danych osobowych słuchaczy UTW. Oba pomieszczenia są wyposażone w szafy drewniane zamykane, przeznaczone również do gromadzenia i przechowywania dokumentacji w formie papierowej. Szafy zamykane są na zwykłe zamki, pomieszczenia nie pozostają bez nadzoru, osoby niepowołane nie mają do nich dostępu.

Dostęp do pomieszczeń i klucze posiada Sekretarka i Prezes Zarządu. W wyznaczonych godzinach urzędowania wstęp do pomieszczenia SEKRETARIATU mają członkowie SUTW oraz słuchacze UTW w celach informacyjno-obsługowych. Wstęp do pomieszczeń mają również wykładowcy przed wykładami, w celach urzędowych – podpisanie dokumentów finansowych, garderoba. W czasie rekrutacji słuchaczy UTW do SEKRETARIATU mają również osoby z zewnątrz – tylko w godzinach urzędowania.

Poza godzinami urzędowania pomieszczenia SUTW są chronione systemem alarmowym chroniącym cały obiekt PCKU. Pomieszczenia SUTW dysponują własnym kodem dostępowym, znanym tylko osobom posiadającym klucze do pomieszczeń. Obiekt PCKU jest chroniony przez Agencję Ochrony Osób i Mienia Grupa Maryt. Rezerwowy klucz dostępu w nagłych przypadkach jest przechowywany i znajduje się pod nadzorem Administratora budynku, tj. PCKU.

Drugim miejscem przetwarzania danych jest stałe miejsce pracy KSIĘGOWEJ, zatrudnionej w SUTW na zasadzie umowy zlecenia. Stałym miejscem pracy Księgowej jest **I Liceum Ogólnokształcące im. Stanisława Staszica w Chrzanowie** 32-500 **Chrzanów, ul. Piłsudskiego 14**, w zespole budynków szkolnych. Właścicielem obiektu jest Starostwo Powiatowe, jest to budynek wielokondygnacyjny, w którym Księgowa pracuje wraz z innymi osobami w pomieszczeniach biurowych z jednym wejściem, zlokalizowanych na parterze. Do pomieszczenia prowadzą z korytarza głównego drzwi PCV, z dwoma zamkami, zabezpieczone metalową kratą. Drzwi nie są plombowane, okna nie są okratowane. Księgowa dysponuje systemem komputerowym (własność SUTW) składającym się z laptopa, korzysta ze szkolnej drukarki wielofunkcyjnej. W laptopie gromadzone są m.in. dane pracowników SUTW i są przetwarzane dla celów płatniczo-fiskalnych. Pomieszczenia są wyposażone w szafy drewniane zamykane, przeznaczone również do gromadzenia i przechowywania dokumentacji w formie papierowej. Szafy zamykane są na zwykłe zamki, pomieszczenia nie pozostają bez nadzoru, osoby niepowołane nie mają do nich dostępu. Dostęp do

pomieszczeń posiadają upoważnieni pracownicy biura Księgowości, dysponujący kluczami (upoważnienie Dyrektora I LO). Klucze rezerwowe znajdują się u Dyrektora I LO. W wyznaczonych godzinach urzędowania wstęp do pomieszczenia mają interesanci w celach informacyjno-obsługowych. Poza godzinami urzędowania pomieszczenia są zamknięte. Obiekty Liceum chronione są systemem alarmowym przez Agencję Ochrony Osób i Mienia ERA.

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe oraz sposób zabezpieczeń poszczególnych budynków, pomieszczeń lub ich części obejmuje dokumentacja prowadzona przez Administratora Danych Osobowych, zgodnie z wzorem stanowiącym odpowiednio Załącznik Nr 5A i 5B do niniejszej Polityki.

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

W Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie przetwarza się dane osobowe we własnej bazie danych utworzonej w formie elektronicznej w programie EXCEL. Dotyczy to następujących zbiorów danych osobowych:

1. Ewidencja słuchaczy Uniwersytetu Trzeciego Wieku w Chrzanowie,
2. Księga słuchaczy UTW.

Dane osobowe słuchaczy UTW, przetwarzane w formie elektronicznej, obejmują następujący zakres, wynikający z Karty zgłoszenia słuchacza i pokwitowania wpłaty:

- ✓ oznaczenie roku akademickiego i semestru,
- ✓ numer porządkowy,
- ✓ nazwisko i imię,
- ✓ data urodzenia,
- ✓ pełny adres zamieszkania,
- ✓ kod identyfikacyjny,
- ✓ numer telefonu stacjonarnego i/lub komórkowego,
- ✓ oznaczenie płci (K lub M),
- ✓ oznaczenie poziomu wykształcenia (w, s, z),
- ✓ oznaczenie statusu zawodowego (e, r, b, p),
- ✓ potwierdzenie wniesienia opłaty (z, -)

Księga słuchaczy UTW – przetwarzana w formie elektronicznej, obejmuje następujący zakres:

- ✓ numer porządkowy,
- ✓ nazwisko i imię,
- ✓ kod identyfikacyjny,
- ✓ uwagi – np. rezygnacja, odszedł (śmierć), odebrał indeks.

3. Dane osobowe pracowników SUTW, zatrudnionych na podstawie umowy zlecenia lub umowy o dzieło, w zakresie płacowo-rozliczeniowym są przetwarzane w formie papierowej i elektronicznej.

Do tego celu służy program księgowy LeftHandFK. Jest to program finansowo-księgowy do obsługi rozliczeń na pełnej księgowości. W programie nie ma bazy danych osobowych w tradycyjnym rozumieniu, są to jedynie zaksięgowane zawarte umowy. Program wymaga loginu i hasła dostępu, z narzucaną częstotliwością zmian hasła.

Dane osobowe przetwarzane przez głównego księgowego dotyczą tylko danych niezbędnych do zawarcia umowy – zlecenia, o dzieło, wolontariatu oraz do rozliczenia tych umów zgodnie z obowiązującymi przepisami, rozliczenia z ZUS oraz Urzędem Skarbowym.

Jest to zbiór pojedynczych, indywidualnych umów w oparciu o ewidencję zawierającą:

- ✓ numer porządkowy umowy,
- ✓ nazwisko i imię,
- ✓ nr umowy.

Umowy w formie papierowej są chronione w zamykanej szafie w pomieszczeniu Księgowości. Czas przechowywania Umów – zgodnie z przepisami dokumenty finansów przechowywane są 5 lat, SUTW nie posiada teczek akt osobowych gdyż nie ma zawartych umów o pracę.

Do rozliczeń z Zakładem Ubezpieczeń Społecznych przeznaczony jest program e-Płatnik - ogólnopolski portal służący do rozliczania składek ZUS. Księgowa posiada login i hasło dostępu, z narzuconą przez program częstotliwością zmian hasła.

Do rozliczeń z Urzędem skarbowym w oparciu o PIT-11 wykorzystywany jest program e-Deklaracje. Jest to system udostępniony przez Ministerstwo Finansów umożliwiający przesyłanie drogą elektroniczną rocznych deklaracji podatkowych w efektywnym rozliczaniu z US.

Dane w tych programach są gromadzone, przetwarzane i przechowywane zgodnie z obowiązującymi przepisami, przesyłanie danych rozliczeniowych może nastąpić tylko po ich podpisaniu certyfikatem kwalifikowanym (podpis elektroniczny) lub przez podpis w aplikacji ePUAP.

W formie papierowej przechowywane są również, wraz z raportem kasowym, kopie pokwitowania wpłaty składek członkowskich SUTW i opłaty za uczestnictwo w zajęciach słuchaczy UTW - forma papierowa (kwitariusz – druk ścisłego zarachowania – kopia różowa) - obejmuje zakres wynikający z zastosowanego druku:

- ✓ numer porządkowy pokwitowania,
- ✓ nazwisko i imię,
- ✓ adres zamieszkania,
- ✓ tytuł płatności
- ✓ data wpłaty,
- ✓ kwota wpłaty (cyframi i słownie)
- ✓ popis przyjmującego wpłatę.

4. Uzupełnieniem powyższych informacji są rejestry danych osobowych przetwarzanych w SUTW w formie papierowej. Są to:

1) Dane osobowe członków Stowarzyszenia UTW, w postaci Deklaracji Członkowskiej, obejmujące następujący zakres:
   - ✓ nazwisko i imię,
   - ✓ data urodzenia,
   - ✓ pełny adres zamieszkania,
   - ✓ numer telefonu stacjonarnego i/lub komórkowego,
   - ✓ poziom wykształcenia (wyższe, średnie, zasadnicze),
   - ✓ status zawodowy (emeryt, rencista, bezrobotny, pracujący),
   - ✓ zgoda na przetwarzanie danych osobowych,
   - ✓ zgoda na wykorzystywanie wizerunku,
   - ✓ decyzja Zarządu SUTW o przyjęciu w poczet członków,
   - ✓ zestawienie opłacalności składki członkowskiej.
2) Dane osobowe słuchaczy UTW, w postaci Karty Zgłoszenia Słuchacza, obejmujące następujący zakres:
   - ✓ oznaczenie roku akademickiego i semestru,
   - ✓ nazwisko i imię,

- ✓ data urodzenia,
- ✓ pełny adres zamieszkania,
- ✓ numer telefonu stacjonarnego i/lub komórkowego,
- ✓ poziom wykształcenia (wyższe, średnie, zasadnicze),
- ✓ status zawodowy (emeryt, rencista, bezrobotny, pracujący),
- ✓ deklaracja uczestnictwa w zajęciach,
- ✓ wybór rodzaju lektoratu,
- ✓ wybór rodzaju zajęć ruchowo-warsztatowych,
- ✓ wybór zajęć dodatkowych,
- ✓ zgoda na przetwarzanie danych osobowych,
- ✓ zgoda na wykorzystywanie wizerunku,

3) Księga słuchaczy UTW, obejmująca następujący zakres:
- ✓ numer porządkowy,
- ✓ nazwisko i imię,
- ✓ kod identyfikacyjny,
- ✓ uwagi – np. rezygnacja, odszedł (śmierć), odebrał indeks

4) kopie pokwitowania wpłaty składek członkowskich i opłaty za uczestnictwo w zajęciach - forma papierowa (kwitariusz – druk ścisłego zarachowania - kopia żółta) - obejmuje zakres wynikający z zastosowanego druku:
- ✓ numer porządkowy pokwitowania,
- ✓ nazwisko i imię,
- ✓ adres zamieszkania,
- ✓ tytuł płatności
- ✓ data wpłaty,
- ✓ kwota wpłaty (cyframi i słownie)
- ✓ popis przyjmującego wpłatę.

5) ewidencja uczestników projektów grantowych realizowanych przez SUTW – obejmuje następujący zakres:
- ✓ numer porządkowy,
- ✓ nazwisko i imię,
- ✓ wiek,
- ✓ podpis,

6) ewidencje uczestnictwa w imprezach wypoczynkowo-turystycznych i sportowych z potwierdzeniem wniesienia opłat - obejmuje zakres wynikający każdorazowo z zastosowanego wzoru, zazwyczaj jest to:
- ✓ numer porządkowy,
- ✓ nazwisko i imię,
- ✓ data urodzenia – dla celów ubezpieczenia,
- ✓ adres zamieszkania – j.w.,
- ✓ kwota wpłaty (cyframi).

c) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

W załączniku nr 6 znajduje się rejestr zbiorów danych osobowych przetwarzanych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie, wraz ze wskazaniem zastosowanych programów, zawartości poszczególnych pól informacyjnych i powiązań między nimi.

Z uwagi na specyfikę zatrudnienia pracowników stałych (2 osoby na zasadzie umowy zlecenie - sekretarka i księgowa) oraz pracowników (wykładowcy i instruktorzy) zatrudnionych na warunkach umowy zlecenia lub umowy o dzieło. Zakres przetwarzanych danych jest ograniczony. Dane do rozliczeń finansowo-podatkowych znajdują się w formie papierowej w indywidualnej Umowie, przechowywanej w formie papierowej.

Zakres tych danych obejmuje:

1. imiona i nazwiska,
2. adres zameldowania, zamieszkania i do korespondencji,
3. datę urodzenia,
4. numer ewidencyjny PESEL i NIP,
5. zwolnienia lekarskie,
6. wysokości wynagrodzenia,
7. ilość posiadanych dzieci,
8. informacja o współmałżonku/współmałżonce,
9. nr konta bankowego.

d) sposób przepływu danych pomiędzy systemami

Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie nie posiada własnego systemu informatycznego służącego do przetwarzania danych osobowych. Dane osobowe przetwarzane są przy użyciu edytora tekstu (MS Word) lub arkusza kalkulacyjnego (MS Excel).

W zakresie zewnętrznych (obcych) systemów informatycznych w SUTW użytkowany jest program księgowy LeftHandFK, program e-płatnik – ogólnodostępna aplikacja ZUS z loginowo-hasłowym dostępem, wysłanie dokumentów do ZUS następuje po weryfikacji przez aplikację e-PUAP, którą dysponuje księgowa oraz program e-Deklaracje do rozliczeń z Urzędem Skarbowym, w którym wysłanie dokumentów następuje po podpisaniu podpisem elektronicznym, którym dysponuje prezes SUTW.

Wykorzystywane systemy informatyczne są systemami odrębnymi i nie współpracują ze sobą.

Podmioty, do których przekazywane są dane to:

a) Zakład Ubezpieczeń Społecznych - elektronicznie,
b) Urząd Skarbowy – elektronicznie,
c) firmy ubezpieczające – w przypadku wyjazdów ubezpieczanych dodatkowo - papierowo,
d) grantodawcy – wg odrębnych wymagań – papierowo lub elektronicznie.

Przelewy finansowe nie są realizowane za pośrednictwem Internetu. Dokumenty są dostarczane do banku w formie papierowej.

e) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych:

Środki organizacyjne:

Do zastosowanych przez Administratora Danych i osoby przez niego upoważnione w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie, środków organizacyjnych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należy:

- ✓ opracowanie i wdrożenie „Polityki bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie”,
- ✓ nadanie przez AD członkom organów SUTW i pracownikom upoważnień do przetwarzania danych osobowych,

- ✓ nadawanie przez AD pracownikom SUTW upoważnień do przetwarzania danych osobowych w związku z realizacją projektów/zadań, w których SUTW będzie realizatorem lub partnerem,
- ✓ nadawanie przez AD pracownikom SUTW upoważnień do przetwarzania danych osobowych w pozostałych przypadkach przetwarzania danych osobowych występujących w SUTW,
- ✓ sprawowanie przez AD kontroli i nadzoru nad procesem wprowadzania danych osobowych do zbioru oraz ich udostępniania.

Osobami upoważnionymi do przetwarzania danych osobowych w organizacji są:

1. sekretarka SUTW,
2. skarbnik SUTW,
3. księgowa SUTW,
4. członkowie Zarządu SUTW.

Powyższy wykaz osób upoważnionych do przetwarzania danych osobowych w organizacji nie ma charakteru zamkniętego i może zostać poszerzony o nowe stanowiska w razie wystąpienia uzasadnionej konieczności.

Dla potrzeb ochrony danych osobowych przetwarzanych w organizacji w formie papierowej stosuje się zabezpieczenia polegające na przechowywaniu:

- ✓ dokumentacji bieżącej w szafach zamykanych na zamki w obszarach przetwarzania danych osobowych,
- ✓ dokumentacji archiwalnej i dokumentacji pracowniczej w specjalnie do tego celu wydzielonej zamykanej szafie w pomieszczeniu Biura Prezesa.

Środki techniczne:

Do zastosowanych przez AD w SUTW środków technicznych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należy:

1. W przypadku zewnętrznych (obcych) systemów informatycznych dla potrzeb bieżącego użytkowania i przesyłania danych stosowane są zabezpieczenia podmiotów, którym przekazywane są dane:

- ✓ W zakresie zewnętrznych (obcych) systemów informatycznych w SUTW użytkowany jest program księgowy LeftHandFK, program e-Płanik – ogólnodostępna aplikacja ZUS z loginowo-hasłowym dostępem, oraz program e-Deklaracje do rozliczeń z Urzędem Skarbowym. Częstotliwość zmian hasła dostępu jest wymuszana przez stosowane programy - program przypomina o upływie terminu ważności hasła, gwarancję zachowania poufności danych stanowi także ograniczenie kręgu osób upoważnionych do jego obsługi – praktycznie jest to tylko Księgowa.
- ✓ Przelewy bankowe są realizowane poprzez dostarczanie dokumentów do banku w formie papierowej, gwarancję zachowania poufności danych stanowi ograniczony krąg osób upoważnionych do popisywania dokumentów bankowych (wg Statutu §32 p.1 - „Do składania oświadczeń woli w imieniu Stowarzyszenia, w tym do zaciągania zobowiązań, zawierania umów i udzielania pełnomocnictw w imieniu Stowarzyszenia uprawnionych jest dwóch członków Zarządu działających łącznie, w tym Prezes lub Skarbnik").

Dostęp do danych osobowych przetwarzanych w systemach informatycznych chroniony jest poprzez:

a) zastosowanie loginów i haseł uniemożliwiających nieuprawnione korzystanie osobom nieupoważnionym,

b) ustawienie monitorów komputerów w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

Loginy i hasła umożliwiające dostęp do komputerów SUTW (sekretariat, księgowa) znajdują się w zapieczętowanych kopertach, przechowywanych w zamykanej szufladzie biurka Prezesa Zarządu.

W przypadku wystąpienia konieczności uzyskania dostępu do któregoś z komputerów w czasie nieobecności pracownika użytkującego komputer, AD może otworzyć zapieczętowaną kopertę i umożliwić wykonanie niezbędnych czynności innemu pracownikowi. Po powrocie pracownika użytkującego dany komputer zmianie ulega hasło dostępu, a zdarzenie takie jest każdorazowo dokumentowane Raportem o naruszeniu ochrony danych osobowych (załącznik nr 7). Raporty przechowywane są w skoroszycie w zamykanej szafie w Biurze Prezesa.

2. W SUTW dla ochrony danych osobowych przetwarzanych w edytorach tekstu (MS Word), arkuszach kalkulacyjnych (MS Excel) lub programach równorzędnych stosowany jest program antywirusowy Avast Free; w systemie informatycznym Księgowej do ochrony systemu informatycznego stosowany jest również program antywirusowy Avast Free.

3. Elektroniczne przetwarzanie danych osobowych odbywa się na laptopach. W związku z chronieniem dostępu do pomieszczeń, w których są one użytkowane, nie podjęto dodatkowych działań ograniczających ryzyko dostania się ich zawartości w niepowołane ręce. Laptopy są zabezpieczone hasłami, a pracownicy i współpracownicy SUTW zostali zapoznani z „Polityką bezpieczeństwa" i przeszkoleni w zakresie ochrony danych osobowych (załącznik 8"A" i 8„B".

f) pozostałe informacje

W SUTW nie są przetwarzane – poza uzasadnionymi przepisami prawa przypadkami przetwarzania danych o stanie zdrowia pracownika – dane wrażliwe (sensytywne).

Kandydaci do udziału w projekcie/zadaniu realizowanym przez SUTW wyrażają pisemnie swoją zgodę na przetwarzanie swoich danych osobowych w związku z prowadzoną rekrutacją do projektu/zadania realizowanego przez organizację dwukrotnie – w Karcie Zgłoszenia po zapoznaniu się z Klauzulą informacyjną oraz poprzez złożenie podpisu na wykazie uczestników projektu. Klauzula nie obejmuje danych wrażliwych, zatem nie mogą one być przetwarzane.

Prawa osób – pracowników SUTW, członków SUTW oraz słuchaczy UTW – są chronione. Każdy z nich potwierdza zapoznanie się ze swoimi prawami w zakresie przetwarzania danych po zapoznaniu się z Klauzulą informacyjną RODO.

Rozdział 2. Przetwarzanie danych osobowych w projekcie/zadaniu, w którym SUTW jest partnerem

Stowarzyszenie Uniwersytet Trzeciego Wieku w Chrzanowie może być partnerem w projekcie/zadaniu realizowanym przez inną instytucję bądź organizację pozarządową.

Jako partner projektu/zadania SUTW będzie realizowało zadania określone w treści stosownego porozumienia dotyczącego realizacji projektu/zadania.

Pracownicy lub członkowie SUTW, realizujący zadania przypisane w treści porozumienia, otrzymują od AD pisemne upoważnienia do przetwarzania danych osobowych w zakresie określonym w treści tych upoważnień niezależnie od tego, czy lider projektu/zadania (realizator) udzielił takiego upoważnienia, czy też nie.

Upoważnienia do przetwarzania danych osobowych udzielane będą odrębnie dla każdego projektu/zadania, w którym SUTW będzie partnerem i będą obowiązywały do dnia ich odwołania.

Do udzielenia upoważnienia do przetwarzania danych osobowych w projekcie/zadaniu, w którym SUTW jest partnerem, stosuje się odpowiednio Załącznik nr 1 „A" do niniejszej „Polityki bezpieczeństwa".

Do odwołania udzielonego upoważnienia stosuje się odpowiednio Załącznik nr 2 do ww. dokumentu.

Do udzielania oraz odwoływania upoważnień do przetwarzania danych osobowych w projekcie/zadaniu, w którym SUTW będzie partnerem upoważniony jest AD.

Miejscem przetwarzania danych osobowych w projekcie/zadaniu, w którym SUTW będzie partnerem będzie siedziba realizatora projektu/zadania.

Rozdział 3. Opis zdarzeń naruszających ochronę danych osobowych

1. Podział zagrożeń:
   1) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu – ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
   3) Zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych – zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy.

      Zagrożenia te możemy podzielić na:

      a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),

      b) nieuprawniony dostęp do systemu z jego wnętrza,

      c) pogorszenie jakości sprzętu i oprogramowania,

      d) bezpośrednie zagrożenie materialnych składników systemu.

      e) nieuprawniony świadomy przekaz danych:
      - ujawnienie loginu i hasła do systemu informatycznego osobom z zewnątrz,
      - udostępnianie stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
      - udostępnianie osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
      - używanie oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
      - przenoszenie programów komputerowych, dysków twardych z jednego stanowiska na inne,
      - kopiowanie danych na nośniki informacji, kopiowanie na inne systemy celem wyniesienia ich poza SUTW,
      - samowolne instalowanie i używanie jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego,
      - używanie nośników danych udostępnionych przez osoby postronne,
      - otwieranie załączników i wiadomości poczty elektronicznej od nieznanych „niezaufanych" nadawców,

- używanie nośników danych niesprawdzonych niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą,
- wykorzystywanie sieci komputerowej w celach innych, niż zgodnie z przeznaczeniem,
- tworzenie kopii zapasowych nie chronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania,
- wyrzucanie dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia uniemożliwiającego ich odtworzenie,
- pozostawianie dokumentów na biurku po zakończonej pracy, pozostawianie otwartych dokumentów na ekranie monitora bez blokady konsoli,
- ignorowanie nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,

f) nieuprawniony nieświadomy przekaz danych:

- zapominanie o wylogowaniu się z systemu komputerowego przed opuszczeniem pomieszczenia,
- złe ustawienie monitora komputerowego, które umożliwia wgląd osobom postronnym,
- pozostawianie bez nadzoru osób trzecich przebywających w pomieszczeniach SUTW, w których przetwarzane są dane osobowe,
- pozostawienie zewnętrznych nośników informacji podłączonych do komputera np. pamięć flash, dyskietki i płyty w napędzie,
- zapisywanie na kartkach i pozostawianie haseł w miejscach widocznych dla innych osób,
- pozostawianie dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach lub w centrach wydruku,
- pozostawianie kluczy w drzwiach, szafach, biurkach, zostawianie otwartych pomieszczeń, w których przetwarza się dane osobowe.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:

1) **sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu**, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
2) **niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
3) **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż;
4) **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5) **pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego** wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
6) **naruszenie lub próba naruszenia** integralności systemu lub bazy danych w tym systemie;

7) stwierdzona **próba modyfikacji lub modyfikacja danych lub zmiana** w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
8) **niedopuszczalna manipulacja** danymi osobowymi w systemie;
9) **ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
10) **nieprzypadkowe odstępstwa od zasad bezpieczeństwa pracy w systemie** wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze osoby, która nie jest formalnie dopuszczona do jego obsługi;
11) **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;
13) **rażące naruszenie dyscypliny pracy** w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), USB, CD w formie niezabezpieczonej itp.

Rozdział 4. Zabezpieczenie danych osobowych

1. Administratorem danych osobowych zawartych i przetwarzanych w rejestrach zbiorów danych Stowarzyszenia Uniwersytet Trzeciego Wieku w Chrzanowie – przedstawionych w Rozdziale 1 podpunkt „b" niniejszej „Polityki bezpieczeństwa" – w systemach informatycznych i na nośnikach tradycyjnych wyszczególnionych w punktach jest Zarząd SUTW.

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych i na nośnikach tradycyjnych, a w szczególności do:

1) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,
2) zapobiegania kradzieży danych,
3) zapobiegania przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

1) przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach;
2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt 1;
3) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji i nośników danych.

4. Do zastosowanych środków organizacyjnych należą następujące zasady:

1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed jej przystąpieniem do pracy przy przetwarzaniu danych osobowych;

2) przeszkolenie osób, o których mowa w pkt 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych;
3) kontrolowanie otwierania i zamykania pomieszczeń wymienionych w pkt 3.1, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę i niepozostawianiu pomieszczenia w czasie pracy bez nadzoru.

5. Niezależnie od niniejszych zasad, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie, przy czym dokumenty te nie mogą być sprzeczne z regulacjami określonymi w „Polityce bezpieczeństwa".

6. AD sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

7. Ochrona danych osobowych przetwarzanych w formie elektronicznej.

1) system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;
2) stosuje się mechanizmy kontroli dostępu do danych osobowych, wprowadzając w tym systemie, rejestrowany dla każdego użytkownika odrębny identyfikator. Dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia przez wprowadzenie hasła;
3) dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed utratą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej przez wykonywanie kopii zapasowych zbiorów danych. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Usuwa się je niezwłocznie po ustaniu ich użyteczności;
4) urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji należy wcześniej pozbawić zapisów tych danych; w przypadku, gdy nie jest to możliwe, uszkodzić w sposób uniemożliwiający ich odczytanie;
5) pracownik SUTW użytkujący komputer przenośny zawierający dane osobowe powinien zachować szczególną ostrożność podczas jego transportu i przechowywania poza obszarem przetwarzania danych osobowych, po odpowiednio uzyskanej zgodzie.

8. Ochrona danych osobowych przetwarzanych w formie papierowej.

Dane osobowe przetwarzane i gromadzone przy użyciu tradycyjnych środków papierowych gromadzone są w rejestrach, księgach, skoroszytach oraz segregatorach. Dane te należy przechowywać w zamykanych szafach.

Obszar przetwarzania i gromadzenia danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych. Przebywanie osób nieupoważnionych w obszarze przetwarzania danych jest dopuszczalne za zgodą AD w obecności osób upoważnionych do przetwarzania danych osobowych.

Sposób postępowania z kluczami do pomieszczeń i szaf został opisany w punkcie poświęconym ochronie fizycznej pomieszczeń, w których przetwarza się dane osobowe.

9. Procedury nadawania uprawnień do przetwarzania danych osobowych.

Do przetwarzania danych, zgodnie z art. 37 ustawy, mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez AD. AD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (załącznik 1 „B"), która zawiera:

1) Imię i nazwisko osoby upoważnionej;
2) Datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
3) Identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Wzór upoważnienia do przetwarzania danych osobowych stanowi Załącznik Nr 1 „A" do niniejszej Polityki.

Dopuszcza się możliwość upoważniania do przetwarzania danych osobowych osób będących pracownikami SUTW w przypadkach i na zasadach przedstawionych w Rozdziale 2.

10. Ochrona fizyczna pomieszczeń, w których przetwarzane są dane osobowe.

1) Budynki i pomieszczenia, w których przetwarzane są dane osobowe, są zabezpieczone w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym, na czas nieobecności osób upoważnionych;
2) Pomieszczenia i budynki, lub ich części, o których mowa w ust. 1 mają zabezpieczenia opisane w Rozdziale 1 pkt. a.

Klucze do szaf na dokumenty, należy przechowywać w danym pomieszczeniu w zamkniętej kasetce. Klucz do kasetki przechowuje pracownik tego pomieszczenia w znanym tylko sobie miejscu. Po zakończeniu pracy osoby odpowiedzialne za pomieszczenia, w których są przetwarzane dane osobowe, są obowiązane sprawdzić zamknięcie szaf i pomieszczeń.

AD zobowiązany jest do prowadzania oraz bieżącej aktualizacji dokumentacji związanej z ochroną danych osobowych zgodnie z wzorem aktualizacji stanowiącym Załącznik Nr 9 do niniejszej Polityki Bezpieczeństwa.

11. Udostępnianie danych osobowych instytucjom spoza SUTW może odbywać się wyłącznie za pośrednictwem i zgodą AD, zgodnie z przepisami ustawy. Warunki udostępnienia danych osobowych omówiono w Części I pkt. 3.

12. W Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie nie występują zbiory wymagające rejestracji u Generalnego Inspektora DO.

13. Rejestr zbiorów danych osobowych przetwarzanych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie zawiera załącznik nr 6, jego zawartość została zdefiniowana w Rozdziale 1 pkt. c. Rejestr prowadzony jest w postaci papierowej lub elektronicznej. Za prowadzenie rejestru i jego aktualizację odpowiada AD. Wpisu do rejestru dokonuje się niezwłocznie po zaistnieniu zdarzenia, powodującego obowiązek dokonania wpisu. Odpowiedni wpis wnosi się również w Arkuszu aktualizacji - załącznik 9.

Rozdział 5. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia:

- ✓ naruszenia zabezpieczeń systemu informatycznego,
- ✓ naruszenia technicznego stanu urządzeń,
- ✓ naruszenia zawartości zbioru danych osobowych,
- ✓ ujawnienia metody pracy lub sposobu działania programu,
- ✓ jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,

- ✓ innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

<u>każda osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana niezwłocznie powiadomić o tym fakcie AD.</u>

2. W razie niemożliwości zawiadomienia AD lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia danych osobowych AD lub upoważnionej przez niego osoby, należy:

- ✓ niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia jeżeli istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych;
- ✓ udokumentować wstępnie zaistniałe naruszenie;
- ✓ nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia AD lub osoby przez niego upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, AD lub osoba przez niego upoważniona:

- ✓ zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji;
- ✓ może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
- ✓ nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza SUTW.

5. Po wyczerpaniu niezbędnych środków doraźnych, związanych z zaistniałym naruszeniem/ ujawnieniem ochrony danych osobowych, AD zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

6. AD dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport – załącznik nr 7, który powinien zawierać w szczególności:

a) wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych;

b) określenie czasu i miejsca naruszenia/ujawnienia i powiadomienia o tym fakcie;

c) określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia;

d) wyszczególnienie wziętych pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;

e) wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia;

f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

7. Zaistniałe naruszenie/ujawnienie ochrony danych osobowych może stać się przedmiotem szczegółowej analizy prowadzonej przez AD.

9. Analiza, o której mowa w pkt. 7, powinna zawierać: wszechstronną ocenę zaistniałego naruszenia/ujawnienia ochrony danych osobowych, wskazanie odpowiedzialnych, wnioski o ewentualnych przedsięwzięciach zaradczo-naprawczych - proceduralnych, organizacyjnych, kadrowych i technicznych, mających na celu zapobieganie podobnym naruszeniom/ujawnieniom w przyszłości.

Rozdział 6. Postanowienia końcowe

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która po stwierdzeniu naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie AD.

2. Osoby, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt poprzez podpisanie oświadczenia (załącznik nr 8 „A" do „Polityki bezpieczeństwa").

3. Ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, zawiera Lista prowadzona przez AD (załącznik nr 8 „B" do „Polityki bezpieczeństwa").

4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie.

5. Orzeczona kara wobec osoby uchylającej się od powiadomienia AD nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz. U. z 1997 r. Nr 133, poz. 883; tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej przez organizację sprawy z powództwa cywilnego o zrekompensowanie poniesionych strat.

6. Wszystkie regulacje dotyczące systemów informatycznych określone w „Polityce bezpieczeństwa" dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

7. Wdrożenie „Polityki bezpieczeństwa" odbywa się poprzez zapoznanie osób wchodzących w skład organów SUTW i pracowników SUTW z treścią „Polityki bezpieczeństwa", a także odpowiedniego szkolenia z zakresu ochrony danych osobowych.

8. „Polityka bezpieczeństwa" wchodzi w życie z dniem podjęcia Uchwały Zarządu SUTW lub w terminie określonym w treści tej Uchwały. Zmiany w „Polityce bezpieczeństwa" będą wchodzić w życie w terminach określonych w Uchwałach Zarządu SUTW dotyczących wprowadzenia zmian w dokumencie. Zmiany te dokumentuje się w Arkuszu Zmian.

Rozdział 7. Arkusz zmian

L.p.	Treść zmiany	Data
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		

CZĘŚĆ II

Instrukcja w sprawie zasad postępowania przy przetwarzaniu danych osobowych

§ 1

Instrukcja w sprawie zasad przetwarzania danych osobowych – zwana dalej „Instrukcją" – określa w szczególności:

1) Obowiązki osób upoważnionych do przetwarzania danych osobowych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie (zwanym dalej „SUTW").

2) Tryb udzielania upoważnień do przetwarzania danych osobowych.

3) Sposób prowadzenia i aktualizacji ewidencji osób upoważnionych do przetwarzania danych osobowych.

4) Sposób prowadzenia i aktualizacji rejestru zbiorów danych osobowych.

§ 2

Definicje zawarte w dokumencie pn.: „Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Uniwersytet Trzeciego Wieku w Chrzanowie" stosuje się odpowiednio.

§ 3

AD sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych zapewniając bezpieczeństwo danych osobowych w systemie informatycznym, w szczególności przeciwdziałając dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz podejmując odpowiednie działania w przypadku wykrycia naruszeń w systemie zabezpieczeń.

§ 4

AD zobowiązany jest do nadzoru nad postępowaniem przy przetwarzaniu danych osobowych w organizacji, a w szczególności do:

1) zastosowania niezbędnych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych, a w szczególności zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, kradzieżą, przetwarzaniem z naruszeniem przepisów prawa, zmianą, utratą, uszkodzeniem lub zniszczeniem.

2) kontroli nad wykonywaniem operacji przetwarzania danych osobowych przez osoby upoważnione.

§ 5

Osoba upoważniona do przetwarzania danych zobowiązana jest do:

1) zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych,

2) zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesu osób, których dane dotyczą,

3) stosowania określonych przez AD procedur i środków przetwarzania oraz zabezpieczania danych osobowych,

4) podporządkowania się poleceniom AD w zakresie ochrony danych osobowych,

5) zachowania danych osobowych w tajemnicy,

6) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa, a w szczególności:
   a) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem,
   b) zabezpieczenia danych osobowych przed ich zmianą,
   c) zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym,
   d) zamykania i zabezpieczania pomieszczeń, w których przetwarzane są dane osobowe w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym,

e) dopilnowania, by przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej,
f) dopilnowania, by przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie,
g) przetwarzania danych osobowych zgodnie z celem, dla którego zostały zebrane,

§ 6

W przypadku stwierdzenia naruszenia zasad postępowania przy przetwarzaniu danych osobowych lub naruszeniu zabezpieczenia danych osoba upoważniona zobowiązana jest niezwłocznie poinformować AD.

§ 7

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez AD.
2. AD ponosi odpowiedzialność za zaznajomienie pracownika, który ma być dopuszczony do przetwarzania danych osobowych, z przepisami towarzyszącymi ochronie danych osobowych. Fakt zapoznania się z przepisami pracownik potwierdza własnoręcznym podpisem.
3. AD wydaje upoważnienia do przetwarzania danych osobowych organom SUTW, każdemu pracownikowi, współpracownikowi, który przy wykonywaniu powierzonych mu zadań przetwarza dane osobowe.
4. Upoważnienie udzielane jest na czas wykonywania przez osobę upoważnioną czynności na powierzonym stanowisku.

§ 8

1. Każda osoba upoważniona powinna odbyć szkolenie z zakresu ochrony danych osobowych.
2. Udział w szkoleniu z zakresu ochrony danych osobowych organizuje AD.

§ 9

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest w formie papierowej i/lub elektronicznej.
2. Ewidencję, o której mowa w pkt. 1, prowadzi AD.
3. Za aktualizację ewidencji osób upoważnionych do przetwarzania danych osobowych odpowiada AD.
4. O każdym zdarzeniu powodującym konieczność wprowadzenia zmian w ewidencji, o której mowa w pkt. 1, musi zostać poinformowany AD.

§ 10

1. **Rejestr zbiorów danych osobowych** przetwarzanych w organizacji prowadzony jest w formie papierowej i/lub elektronicznej.
2. Rejestr zbiorów danych osobowych prowadzi AD.
3. O potrzebie utworzenia nowego zbioru danych osobowych pracownik wnioskuje do AD. Wniosek powinien zawierać:
a) nazwę zbioru,
b) podstawę utworzenia zbioru,
c) oznaczenie rodzaju zbioru,
d) określenie sposobu przetwarzania danych w zbiorze (system informatyczny, przetwarzanie elektroniczne, przetwarzanie odręczne),
e) określenie zakresu przetwarzania danych,
f) określenie celu przetwarzania danych,
g) informację o kategoriach odbiorców, którym dane mogą być przekazywane,
h) informację o sposobie udostępniania danych,

i) informację o tym, czy zbiór podlega obowiązkowi rejestracji przez Generalnego Inspektora Ochrony Danych Osobowych,

j) uzasadnienie potrzeby utworzenia zbioru.

4. O każdej zmianie dotyczącej przetwarzania danych w zbiorze należy poinformować AD.

CZĘŚĆ III

Instrukcja dla osób upoważnionych do przetwarzania danych osobowych

§ 1

Niniejsza „Instrukcja dla osób upoważnionych do przetwarzania danych osobowych" – zwana dalej „Instrukcją" – określa tryb postępowania w przypadku, gdy:

- ✓ stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie.
- ✓ stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 2

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:

1) **Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu**, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej, itp.

2) **Niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych.

3) **Awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż.

4) **Pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.

5) **Jakość danych w systemie lub inne odstępstwo** od stanu oczekiwanego wskazuje na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.

6) **Nastąpiło naruszenie lub próba naruszenia** integralności systemu lub bazy danych w tym systemie.

7) **Stwierdzono próbę lub modyfikację danych lub zmianę** w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).

8) **Nastąpiła niedopuszczalna manipulacja danymi osobowymi** w systemie.

9) **Ujawniono osobom nieupoważnionym dane osobowe** lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń.

10) **Praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa** od założonego rytmu pracy, wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.

11) **Ujawniono istnienie nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki", itp.

12) **Podmieniono lub zniszczono nośniki z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe.

13) **Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

§ 3

1. Każda osoba w SUTW (reprezentująca organ SUTW bądź w niej zatrudniona), która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym lub przetwarzanych w inny sposób, powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu tych danych, bezpośredniego przełożonego oraz AD albo inną upoważnioną przez niego osobę.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych zobowiązana jest niezwłocznie powiadomić o tym AD.

§ 4

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.
2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa – należy przeprowadzić postępowanie wyjaśniające czy te dane osobowe należy uznać za ujawnione.

§ 5

Niezwłocznie po uzyskaniu informacji o naruszeniu danych osobowych należy podjąć działania w celu powstrzymania lub ograniczenia dostępu do danych przez osoby niepowołane poprzez:

1) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej,
2) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
3) zmianę hasła na konto AD i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
4) podjęcie innych – stosownych do zagrożenia – działań.

§ 6

AD – po uzyskaniu sygnału o naruszeniu danych osobowych – powinien w pierwszej kolejności:

1) zapisać wszelkie informacje związane z danym zdarzeniem,
2) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
3) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia – zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby nieuprawnionej,
4) wyniki postępowania zabezpieczającego oraz okoliczności naruszenia bezpieczeństwa danych osobowych należy ująć w raporcie.

§ 7

1. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych AD lub upoważnionej przez niego osoby należy:

1) niezwłocznie podjąć czynności (określone w rozdziale 6 pkt. 3 niniejszej „Polityki bezpieczeństwa”) niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych – stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania – jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,

6) zastosować się do innych instrukcji i regulaminów – jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia AD lub upoważnionej przez niego osoby.

2. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych AD lub osoba go zastępująca:
1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy SUTW,
2) niezwłocznie informuje AD,
3) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza SUTW.

§ 8

1. Po dokonaniu czynności zabezpieczenia danych osobowych i ustaleniu przyczyn naruszenia ochrony danych osobowych należy niezwłocznie przywrócić normalny stan działania.
2. Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
3. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych AD niezwłocznie zarządza przeprowadzenie dodatkowego szkolenia dla osób biorących udział przy przetwarzaniu danych osobowych. Dokumentację z przeprowadzonego szkolenia AD załącza do raportu określonego w treści § 9.

§ 9

1. Po dokonaniu czynności przedstawionych powyżej AD sporządza szczegółowy raport zawierający:
1) opis zdarzenia,
2) przyczynę zaistnienia,
3) skutki naruszenia ochrony danych osobowych,
4) podjęte działania, zastosowane środki,
5) analizę zdarzenia oraz wnioski dotyczące przedsięwzięć:
a) organizacyjnych,
b) technicznych,
c) kadrowych.

2. Na podstawie raportu AD wydaje pisemne zalecenia.
3. Całość dokumentacji w zakresie naruszenia systemu ochrony danych osobowych przechowuje AD w formie papierowej lub elektronicznej.

CZĘŚĆ IV

Wykaz załączników

Załącznik nr 1 „A" – wzór Upoważnienia do przetwarzania danych osobowych.

Załącznik nr 1 „B" – wzór Ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 2 – Odwołanie upoważnienia do przetwarzania danych osobowych

Załącznik nr 3 „A" – Klauzula informacyjna członka SUTW

Załącznik nr 3 „B" – Klauzula informacyjna słuchacza UTW

Załącznik nr 3 „C" – Klauzula informacyjna pracownika SUTW

Załącznik nr 4 „A" – Deklaracja członkowska SUTW

Załącznik nr 4 „B" – Karta zgłoszenia słuchacza UTW

Załącznik nr 5 „A" – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Załącznik nr 5 „B" – Sposób zabezpieczenia poszczególnych budynków, pomieszczeń lub ich części

Załącznik nr 6 – Rejestr zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, zawartością poszczególnych pól informacyjnych i powiązań między nimi. Sposób przepływu danych pomiędzy poszczególnymi systemami.

Załącznik nr 7 „A" – Raport z naruszenia ochrony danych osobowych

Załącznik nr 7 „B" – Analiza naruszenia ochrony danych osobowych

Załącznik nr 8 „A" – Oświadczenie o zapoznaniu się z PB

Załącznik nr 8 „B" – Lista osób, które zapoznały się z PB

Załącznik nr 9 – Arkusz aktualizacji.