Polityka Bezpieczeństwa
Ochrony Danych Osobowych

dla

CZĘSTOCHOWSKIEGO CENTRUM ŚWIADCZEŃ

Wersja 1		**Pieczęć firmowa:**	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Tomasz Salachna	2017-03-24		2017-03-24

Spis treści

1. Wstęp....3
2. Definicje....4
3. Zadania ABI ustawowe i scedowane przez ADO....5
4. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe....6
5. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych....6
6. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi....6
7. Sposób przepływu danych pomiędzy poszczególnymi systemami....6
8. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych....6
9. Procedura postępowania z incydentami (Instrukcja alarmowa)....7
10. Procedura działań korygujących i zapobiegawczych....8
11. Sprawdzenie zgodności przetwarzania danych osobowych z przepisami prawa....9
12. Zarządzanie systemem ochrony danych....10
13. Szkolenia lub zapoznawanie osób z zasadami ODO....12
14. Postanowienia końcowe....12

1. Wstęp

Polityka Bezpieczeństwa jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora Danych Osobowych. Została opracowana zgodnie z wymogami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016r. poz. 922) oraz wymaganiami określonymi w §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Opisane i zastosowane w niej zabezpieczenia mają zapewnić:

1. poufność danych - rozumianą, jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. integralność danych - rozumianą, jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność danych - rozumianą, jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. integralność systemu rozumianą, jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

2. Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. Polityka – rozumie się przez to Politykę bezpieczeństwa ochrony danych osobowych
2. Administrator Danych Osobowych (ADO) –Dyrektor Centrum, decydujący o celach i środkach przetwarzania danych osobowych;
3. Administrator Bezpieczeństwa Informacji (ABI) – osoba powołana przez ADO odpowiedzialna za organizację ochrony danych osobowych.
4. Ustawa – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. ochronie danych osobowych
5. Rozporządzenie MSWiA – Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)
6. Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
7. Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;
8. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
9. Zgoda osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
10. Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
11. Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
12. System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
13. Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
14. Użytkownik – osoba posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych lub zleceniem;
15. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,
16. Nośnik komputerowy (wymienny) – nośnik służący do zapisu i przechowywania informacji, np. pendrive, DVD, dyski twarde;

3. Zadania ABI ustawowe i scedowane przez ADO

Do ustawowych obowiązków ABI należy:

1. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
2. nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 UODO, oraz przestrzegania zasad w niej określonych,
3. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
4. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów zawierających dane wrażliwe

Do pozostałych obowiązków ABI scedowanych przez ADO należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami polityki bezpieczeństwa informacji
3. wydawanie i anulowanie Upoważnień do przetwarzania danych osobowych,
4. prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych,
5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

Administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań scedowanych, o których mowa w pkt. 1-4.

Administrator Bezpieczeństwa Informacji ma prawo:

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji
2. wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
3. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,

ABI formalnie powołuje się zgodnie z Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934) oraz z użyciem **Załącznika A Powołanie ABI**.

4. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej, zawierającej dane osobowe, opisane jest w **Załączniku B Wykaz zbiorów danych osobowych**

5. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisany jest w **Załączniku B Wykaz zbiorów danych osobowych**

6. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Opis struktury zbiorów danych osobowych przedstawiono w **Załączniku C Opis pól informacyjnych i powiązań**

7. Sposób przepływu danych pomiędzy poszczególnymi systemami

Sposób przepływu danych osobowych pomiędzy systemami, w których przetwarzane są dane osobowe przedstawiono w **Załączniku D Sposób przepływu danych**

8. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

8.1 Zabezpieczenia organizacyjne

Został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych.

1. została opracowana i wdrożona polityka bezpieczeństwa
2. została opracowana i wdrożona instrukcja zarządzania systemem informatycznym
3. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych
4. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych
5. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego
6. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy
7. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych
8. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych

9. stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe

8.2 Zabezpieczenia fizyczne pomieszczeń z danymi osobowymi w wersji papierowej i elektronicznej.

Zabezpieczenia fizyczne opisane są w **Załączniku B Wykaz zbiorów danych osobowych**

8.3 Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

Są to zabezpieczenia sieci, serwera, sprzętu komputerowego, serwera i systemów operacyjnych. Szczegółowa lista zabezpieczeń zawarta jest w instrukcji zarządzania systemem informatycznym (**Rozdział 4 Instrukcji**)

8.4 Zabezpieczenia narzędzi programowych i baz danych

Są to zabezpieczenia programów i aplikacji przetwarzających dane osobowe. Szczegółowa lista zabezpieczeń zawarta jest w instrukcji zarządzania systemem informatycznym (**Rozdział 5 Instrukcji**)

9. Procedura postępowania z incydentami (Instrukcja alarmowa)

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych lub zobowiązana do zachowania poufności danych osobowych w przypadku stwierdzenia zaistnienia podatności lub wystąpienia incydentu, zobowiązana jest poinformować o tym bezpośredniego przełożonego lub Administratora Bezpieczeństwa Informacji.
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom

nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)

4. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości
    d. dokumentuje prowadzone postępowania
5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały
    b. zabezpiecza ewentualne dowody
    c. ustala osoby odpowiedzialne za naruszenie
    d. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody)
    e. inicjuje działania dyscyplinarne
    f. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości
    g. dokumentuje prowadzone postępowania

10.Procedura działań korygujących i zapobiegawczych

Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych.

1. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami stawy o Ochronie Danych Osobowych, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
2. Osobą odpowiedzialną za nadzór nad procedurą jest Administrator Bezpieczeństwa Informacji.

Definicje

1. **Incydent** - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
2. **Zagrożenie** – potencjalna możliwość wystąpienia incydentu
3. **Korekcja** – działanie w celu wyeliminowania skutków incydentu.
4. **Działanie korygujące** – jest to działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji.
5. **Działanie zapobiegawcze** – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.
6. **Kontrola** – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki i instrukcji.

Opis czynności

1. ABI jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
    a. zgłoszenia od pracowników
    b. wiedza ABI
    c. wyniki kontroli wewnętrznych ODO, kontroli GIODO lub pozostałych
2. W przypadku, gdy ABI stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną
3. ABI jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4. Po przeprowadzeniu działań korygujących lub zapobiegawczych, ABI jest zobowiązany do oceny efektywności ich zastosowania.
5. Powyższe czynności ABI w rejestruje w pliku **Załącznik E - zadania ODO.xls** .

11. Sprawdzenie zgodności przetwarzania danych osobowych z przepisami prawa

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych ze sprawdzaniem zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych (na podstawie rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r., poz. 745)
2. Za przeprowadzenie sprawdzenia odpowiada ABI
3. Sprawdzeniu podlegają: zbiory, systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami U.O.D.O.
4. ABI przygotowuje plan sprawdzeń (możliwy kwartalny lub roczny) uwzględniając zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania **Załącznik F1 – Plan kontroli**. W okresie 5 lat należy dokonać sprawdzenia wszystkich zbiorów i systemów Administratora Danych.
5. ABI jest zobowiązany do przedstawienia ADO planu sprawdzeń najpóźniej na 2 tygodnie przed dniem rozpoczęcia okresu objętego planem.
6. ABI prowadzi sprawdzenia zgodnie z planem lub może wszcząć sprawdzenia doraźne na skutek podejrzenia lub naruszenia ochrony danych osobowych.
7. ABI zobowiązany jest do powiadomienia kierowników kontrolowanych jednostek o sprawdzeniu w terminie co najmniej 7 dni przed jego przeprowadzeniem.
8. Sprawdzenie przeprowadzane jest na podstawie listy kontrolnej dokumentu **Załącznik F2 - lista kontrolna ODO**
9. ABI może dokumentować przebieg sprawdzenia w postaci danych i wydruków z kontrolowanych systemów (programów) oraz poprzez sporządzanie: notatek z czynności, protokołów odebrania ustnych wyjaśnień, protokołów z oględzin, kopii dokumentów, printscreenów, logów systemowych, zapisów konfiguracji technicznych środków zabezpieczeń systemów

10. Po dokonanym sprawdzeniu, ABI przygotowuje i przekazuje do ADO sprawozdanie **Załącznik F3 – Sprawozdanie pokontrolne**. W przypadku sprawdzenia planowego, sprawozdanie powinno być przekazane ADO nie później niż w terminie 30 dni od zakończenia sprawdzenia. W przypadku sprawdzenia doraźnego, sprawozdanie powinno być dostarczone do ADO niezwłocznie po zakończeniu sprawdzenia.

12.Zarządzanie systemem ochrony danych

1. **Procedura trybu i nadzoru nad Polityką i Instrukcją** (na podstawie Rozporządzenia Ministra Administracji i Cyfryzacji (Dz.U. 2015 Poz. 745) z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji
    a. ABI odpowiada za weryfikację Polityki i Instrukcji pod kątem aktualności, kompletności oraz zgodności z przepisami UODO
    b. ABI odpowiada za weryfikację stanu faktycznego przetwarzania danych osobowych przez Administratora Danych
    c. ABI odpowiada za weryfikację skuteczności zabezpieczeń technicznoorganizacyjnych opisanych w Polityce i Instrukcji
    d. ABI odpowiada za weryfikację przestrzegania obowiązków nałożonych na osoby uczestniczące w procesie przetwarzania danych
    e. Weryfikacja realizowana jest poprzez **sprawdzenia**, **wnioski lub nieprawidłowości** zgłaszane przez osoby wykonujące obowiązki określone w Polityce i Instrukcji, poprzez **własne inicjatywy ABI** oraz na **podstawie zgłoszenia osoby trzeciej**
    f. W przypadku wykrycia podczas weryfikacji nieprawidłowości, ABI zawiadamia ADO o nieopracowaniu lub brakach w dokumentacji oraz działaniach podjętych w celu doprowadzenia dokumentacji do stanu zgodnego z przepisami
    g. Jeśli nieprawidłowości dotyczą konkretnych osób, ABI instruuje osoby o prawidłowych procedurach działania, poucza osoby naruszające zasady ODO lub zawiadamia administratora danych, wskazując osobę odpowiedzialną za naruszenie zasad oraz jego zakres
2. **Zarządzanie wewnętrznym rejestrem zbiorów** (na podstawie Rozporządzenia Ministra Administracji i Cyfryzacji (Dz.U. 2015 Poz. 719) z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych)
    a. Prowadzenie rejestru jest wyłączną rolą ABI
    b. W stosunku do każdego zbioru danych w rejestrze dokumentowane są podstawowe dane informacyjne o zbiorze, zgodnie z **Załącznikiem Zalacznik_G_Rejestr_zbiorow_ABI**
    c. ABI jest zobowiązany do wpisu w rejestrze nowego zbioru, odnotowania zmiany informacji w zbiorze oraz odnotowaniu faktu zaprzestania przetwarzania danych w zbiorze (nowy wpis, aktualizacja, wykreślenie);
    d. W przypadku prowadzenia rejestru w postaci elektronicznej, ABI udostępnia rejestr do przeglądania, przez stronę www lub w systemie informatycznym w siedzibie administratora danych
    e. W przypadku prowadzenia rejestru w postaci papierowej, ABI udostępnia każdemu zainteresowanemu jego treść w siedzibie administratora danych

3. **Roczne spotkanie podsumowujące stan ochrony danych osobowych** może organizować ABI, na którym dokonywana jest ocena funkcjonowania systemu ochrony danych osobowych oraz planowane są działania związane z poprawą stanu ochrony danych osobowych. Uczestnikami spotkania są: ABI oraz wybrane osoby odpowiedzialne za stan ochrony danych osobowych w organizacji. a następnie przedstawiany jest najwyższemu kierownictwu. Raport przygotowany jest według **Załącznika_G1_Sprawozdanie_ODO**. i przedkładany ADO.

13.Szkolenia lub zapoznawanie osób z zasadami ODO

1. Każda osoba przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami w wersji papierowej winna być poddana przeszkoleniu lub zapoznana z:
    a. przepisami ustawy o ochronie danych osobowych oraz przepisami wydanych do niej aktów wykonawczych,
    b. zasadami ochrony danych osobowych zawartych w Polityce i Instrukcji,
    c. z zasadami ujętymi w Regulaminie ochrony danych osobowych (patrz załącznik **Regulamin Ochrony Danych Osobowych**).
2. Za przeprowadzenie szkolenia lub zapoznania z zasadami ochrony danych osobowych odpowiada ABI.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą **Załącznika H – Plan szkolenia ODO.**
4. Każda osoba po szkoleniu lub po zapoznaniu z zasadami ochrony danych osobowych zobowiązana jest do podpisania Oświadczenia o poufności (patrz **Załącznik I – Oświadczenie poufności**).
5. Podpisane Oświadczenia poufności powinny być zarchiwizowane, np. w aktach osobowych lub w segregatorze.
6. Oświadczenie poufności stanowi podstawę do nadania upoważnienia do przetwarzania danych osobowych.

14.Postanowienia końcowe

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody ADO
2. Polityka Bezpieczeństwa może być udostępniania osobom i instytucjom postronnym bez zgody ADO, jeżeli nie zawiera w treści informacji o zabezpieczeniach danych osobowych a wszelkie załączniki występują w formie niewypełnionych szablonów
3. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszej Polityce.
4. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
5. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.