Załącznik Nr 1

Do Zarządzenia Nr 5/2015 r.

Kierownika Miejsko-Gminnego Ośrodka

Pomocy Społecznej w Pełczycach

Z dnia 22.09.2015 r.

Polityka bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych

W Miejsko-Gminnym Ośrodku Pomocy Społecznej w Pełczycach

I – Część ogólna

§ 1

Realizując postanowienia ustawy ochronie danych osobowych (t. j. Dz. U. z 2014 r. poz. 1182) oraz wydane w oparciu o deklarację ustawową przepisy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024) , Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji ustanawia się „Politykę bezpieczeństwa danych osobowych i danych wrażliwych w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Pełczycach” , zwaną dalej „Polityką bezpieczeństwa” .

§ 2

Ilekroć w niniejszym dokumencie jest mowa o :

1. Ośrodku ; należy przez to rozumieć Miejsko-Gminny Ośrodek Pomocy Społecznej w Pełczycach,
2. Ustawie ; należy przez to rozumieć ustawę, o której mowa w § 1 niniejszej części,
3. ADO ; należy przez to rozumieć Administratora Danych Osobowych w rozumieniu ustawy, Administratorem danych jest Miejsko-Gminny Ośrodek Pomocy Społecznej w Pełczycach. W imieniu Administratora Danych Osobowych obowiązki określone w Ustawie pełni Kierownik Ośrodka,
4. ABI ; należy przez to rozumieć Administratora Bezpieczeństwa Informacji w rozumieniu Ustawy,
5. ASI ; należy przez to rozumieć Administratora Systemów Informacyjnych .

6. Polityka ; należy przez to rozumieć „Politykę bezpieczeństwa”, obowiązująca w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Pełczycach,
7. Instrukcja ; należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Pełczycach,
8. GIODO ; należy przez to rozumieć „Generalnego inspektora Ochrony Danych Osobowych” ,
9. Sprawdzenie ; należy przez to rozumieć czynności mające na celu zweryfikowanie zgodności przetwarzanych danych osobowych z przepisami o ochronie danych osobowych,
10. Sprawozdanie ; należy przez to rozumieć dokument, o którym mowa w Art. 36c ustawy, opracowany przez ABI po dokonaniu sprawdzenia,
11. Użytkownik systemu ; należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w Ośrodku, osoba wykonująca na podstawie umowy – zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Ośrodku,
12. System informatyczny ; należ przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania informacji ,
13. Przetwarzanie danych ; należy przez to rozumieć jakiekolwiek operacje, wykonywane na danych osobowych, takie jak zbieranie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,
14. Zabezpieczenie danych w systemie informatycznym ; należy przez to rozumieć wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed ich nieuprawnionym przetwarzaniem,
15. Dane osobowe ; danymi osobowymi nie są pojedyncze informacje o dużym stopniu ogólności, np. sama nazwa ulicy i nr domu, w którym mieszka wiele osób. Informacja ta jednak będzie stanowiła dane osobowe wówczas, gdy zostanie zestawiona z innymi, dodatkowymi informacjami, np. imieniem nazwiskiem czy nr PESEL, które w konsekwencji można odnieś do konkretnej osoby,
16. Dane szczególnie chronione ; wyliczone są w art. 27 ust. 1 ustawy. Są to informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych, religijnych, filozoficznych, wyznaniu, przynależności do partii, lub związku, stanie zdrowia, kodzie genetycznym, nałogach, postępowaniu przed sądem lub urzędem. Na administratorów tych danych ustawa nakłada bardziej rygorystyczne obowiązki, niż na administratorów danych zwykłych,
17. Dane „zwykłe” ; nie jest to pojęcie zdefiniowane w ustawie o ochronie danych osobowych. Pojecie to obejmuje dane osobowe poza wymienionymi w art. 27 ust. 1 ustawy. Zalicza się do nich np. imię, nazwisko, adres zamieszkania, datę urodzenia, nr PESEL, adres e-mail,

18. Zgoda na przetwarzanie danych osobowych ; należy przez to rozumieć zgodę osoby, której dane dotyczą – rozumie się oświadczenie woli, którego treścią jat zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli innej treści. Wyrażenie zgody na przetwarzanie danych osobowych jest zbędne, gdy przetwarzanie danych jest dopuszczalne na podstawie : odrębnych przepisów prawa (np. w celu przeprowadzenia wywiadu środowiskowego przez pracownika pomocy społecznej) lub innych przesłanek (np. w celu realizacji umowy) ,
19. Usuwanie danych osobowych ; należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. Usuwanie danych oznacza więc takie procedury, których zastosowanie pozbawi administratora danych możliwości dalszego przetwarzania danych osobowych.

§ 3

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym odpowiadają w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Pełczycach,

a) Administrator Danych Osobowych,
b) Administrator Bezpieczeństwa Informacji,
c) Administrator Systemów Informatycznych,
d) Każda osoba wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz ADO, która uzyskała upoważnienie do przetwarzania danych osobowych.

II – Zasady przetwarzania i ochrony danych osobowych

§ 1

Każda osoba, mająca dostęp do danych osobowych przetwarzanych w Ośrodku jest zobowiązana do zapoznania się z niniejszym dokumentem.

§ 2

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Ośrodek, przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi, jak i zewnętrznymi, świadomymi lub nieświadomymi.

§ 3

Polityką bezpieczeństwa objęte są dane osobowe, którymi zgodnie z ustawą są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

§ 4

Reguły i zasady do przetwarzania danych osobowych prowadzonych zarówno w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych obowiązują także w przypadku przetwarzania danych poza zbiorem danych.

§ 5

Integralną częścią polityki bezpieczeństwa są następujące dokumenty :

1) Wykaz pomieszczeń lub część pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe i dane wrażliwe (Załącznik nr 1).
2) Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (Załącznik nr 2).
3) Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (Załącznik nr 3).
4) Sposób przepływu danych pomiędzy poszczególnymi systemami (Załącznik nr 4).
5) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (Załącznik nr 5).
6) Obowiązki pracownicze osób zatrudnionych przy przetwarzaniu danych osobowych i danych wrażliwych wynikające z potrzeby zapewnienia ochrony danych osobowych (Załącznik nr 6)

§ 6

Osoby, które przetwarzają w Ośrodku dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych osobowych nadane przez ADO (Załącznik nr 7) zawierające oświadczenie o zachowaniu poufności tych danych.

Osoby upoważnione do przetwarzania danych mają obowiązek :

a) Przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem,
b) Nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym,
c) Zabezpieczać je przed zniszczeniem.

§ 7

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jaki mowa w § 6, które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu poufności (Załącznik nr 8).

§8

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych zgodnie z art. 31 ustawy. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§ 9

Udostępnianie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności pisemny wniosek podmiotu uprawnionego. Dane osobowe mogą być udostępnione osobom i podmiotom, zgodnie z przepisami prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

§ 10

Udostępnianie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

- adresat wniosku (ADO),

- wnioskodawca,

- podstawa prawna (wskazanie potrzeby),

- wskazanie przeznaczenia,

- zakres informacji.

§ 11

Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 12

Każda osoba fizyczna, której dane są przetwarzane w Ośrodku, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust. 1 pkt. 7 i pkt. 8 ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

§ 13

W przypadku otrzymania wniosku o udostępnianie danych osobowych od osoby, której one dotyczą, wyznaczona przez ADO osoba przygotowuje odpowiedź do trzydziestu dni od daty wpłynięcia wniosku.

§ 14

W przypadku zbierania danych osobowych od osoby, której one dotyczą, ADO (lub osoba przez niego wyznaczona) jest obowiązany poinformować tę osobę o :

a) Adresie swojej siedziby i pełnej nazwie, a w przypadku, gdy ADO jest osobą fizyczną – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
b) Celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
c) Prawie dostępu do treści swoich danych oraz ich poprawiania,
d) Dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

§ 15

Nadzór nad przetwarzaniem danych osobowych w Ośrodku sprawuje ABI wyznaczony przez ADO. ADO jest zobowiązany zgłosić do rejestracji w GIODO powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od jego powołania lub odwołania. W przypadku niewyznaczenia ABI, funkcje mu przypisane pełni ADO osobiście. Upoważnienie wyznaczające ABI stanowi załącznik nr 9 do niniejszego dokumentu lub zarządzenie kierownika Ośrodka na ten temat. ABI jest zobowiązany do podpisania oświadczenia, stanowiącego załącznik do niniejszego dokumentu.

§ 16

Do zadań ABI należy w szczególności :

a) Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania, które za pośrednictwem administratora danych zostaje przekazane do GIODO,
b) Nadzorowanie opracowania i aktualizowanie dokumentacji opisującej sposób przetwarzania danych osobowych oraz przestrzegania zasad w niej określonych,
c) Zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
d) Prowadzenie rejestru zbioru danych osobowych przetwarzanych przez administratora danych (załącznik nr 10) oraz , kiedy jest to wymagane przez przepisy, zgłaszanie zbiorów do rejestracji do GIODO,

e) Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.

§ 17

ABI prowadzi również następujące wykazy :

a) Ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych (Załącznik nr 11)
b) Wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (załącznik nr 1)
c) Wykaz zbioru danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (załącznik nr 2)
d) Wykaz podmiotów i osób, którym udostępniono dane (załącznik nr 12)
e) Wykaz podmiotów, którym powierzono dane osobowe do przetwarzania (załącznik nr 13) .

§ 18

Nadzór nad przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym sprawuje ASI.

§ 19

Funkcję ASI pełni osoba wyznaczona przez ADO. ADO może każdorazowo odwołać ASI. W przypadku niewyznaczenia ASI obowiązki dla niego przewidziane wykonuje ABI.

§ 20

Do zadań ASI należy w szczególności :

a) Nadzór nad właściwym zabezpieczeniem sprzętu, w którym przetwarzane są dane osobowe,
b) Nadzór nad wykorzystywaniem w Ośrodku oprogramowania i jego legalnością,
c) Przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przechowywane są dane osobowe,
d) Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych,
e) Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
f) Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych,
g) Nadzór nad wykorzystywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem przydatności,

III – Tryb i sposób sprawdzania zgodności przetwarzania danych osobowych z obowiązującymi przepisami

§ 1

Sprawdzanie o którym mowa w § 16 pkt. a części II przeprowadzane jest w trybie :

a) Sprawdzania planowego – wg planu sprawdzeń,
b) Sprawdzenia doraźnego, w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez ABI informacji lub wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takich naruszeń,
c) Zgodnie z art. 19 b ust. 1 Ustawy – w przypadku zwrócenia się o dokonanie sprawdzenia przez GIODO.

§ 2

Plan sprawdzeń określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.

§ 3

ABI w planie sprawdzeń uwzględnia w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych :

a) Z zasadami przetwarzania danych osobowych, których jest mowa w ustawie,
b) Z zasadami dotyczącymi zabezpieczenia danych osobowych, których mowa w ustawie,
c) Z zasadami przekazywania danych osobowych, o których jest mowa w ustawie, z obowiązkiem zgłaszania zbioru danych osobowych do rejestracji i jego aktualizacji, o których mowa w ustawie.

§ 4

Plan sprawozdań jest przygotowywany przez ABI na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

§ 5

Zbiory danych oraz systemy informatyczne służące do przetwarzania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat.

§ 6

Sprawdzanie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez ABI o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

§ 7

ABI zawiadamia ADO o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia w trybie o którym mowa w art. 19 b ust. 1 ustawy, przed podjęciem pierwszej czynności w toku sprawdzania.

§ 8

ABI dokumentuje czynności przeprowadzone w toku sprawdzania, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.

§ 9

Dokumentowanie czynności w toku sprawdzenia może polegać, w szczególności na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na :

a) Sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych,
b) Odebraniu wyjaśnień osoby, której czynności objęto sprawdzaniem,
c) Sporządzeniu kopii otrzymanego dokumentu,
d) Sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych,
e) Sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisu konfiguracji technicznych środków zabezpieczeń tego systemu.

§ 10

W systemie informatycznym służącym do przetwarzania danych osobowych lub ich zabezpieczania , czynności ABI mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych, szczególności osoby zarządzające tym systemem.

§ 11

Materiały są sporządzane w postaci papierowej lub w postaci elektronicznej.

§ 12

Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenia, bierze udział w sprawdzeniu lub umożliwia ABI przeprowadzenie czynności w toku sprawdzenia.

§ 13

ABI zawiadamia ADO o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

§ 14

Zawiadomienie nie przekazuje się w przypadku :

a) Sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzania jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji czy naruszenie miało miejsce,
b) Sprawdzenia, którego dokonanie zwróciło się GIODO, jeżeli na zawiadomienie nie pozwala wyznaczony przez nie termin,

§15

Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie.

§ 16

Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.

§ 17

ABI przekazuje ADO sprawozdanie :

a) Ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia,
b) Ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia,
c) Ze sprawdzenia, o którego dokonanie zwróciło się GIODO – zachowując termin wskazany przez Generalnego Inspektora zgodnie z art. 19 b pkt. 1 ustawy.

§ 18

Nie rzadziej niż raz na rok bezpieczeństwo informacji danych osobowych w Ośrodku poddawane jest audytowi wewnętrznemu zgodnie z obowiązującymi przepisami.

IV – Tryb i sposób nadzoru na dokumentacją przetwarzania danych

§ 1

Sprawując nadzór, ABI dokonuje weryfikacji :

a) Opracowania i kompletność dokumentacji przetwarzania danych,
b) Zgodności dokumentacji przetwarzania danych osobowych z obowiązującymi przepisami prawa,
c) Stanu faktycznego w zakresie przetwarzania danych osobowych,
d) Zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych,
e) Przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

§ 2

ABI przeprowadza weryfikację :

a) W sprawdzeniach
b) Poza sprawdzeniami, na podstawie zgłoszenia osoby wykonującej obowiązki określone w dokumentacji przetwarzania danych osobowych oraz własnego udziału ABI w procedurach w niej określonych.

§ 3

ABI może przeprowadzić weryfikację poza sprawdzeniami, na podstawie zgłoszenia osoby trzeciej.

V – Instrukcja alarmowa (postępowanie w przypadku naruszenia ochrony danych osobowych)

§ 1

Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą :

a) Próby naruszenia ochrony danych osobowych :
   - z zewnątrz – włamania do systemu, podsłuch, kradzież danych,
   - z wewnątrz – nieumyślna lub celowa modyfikacja danych, kradzież danych.
b) programy destrukcyjne :
   - wirusy
   - konie trojańskie
   - makra
   - bomby logiczne
c) awarie sprzętu lub oprogramowania,
d) zabór sprzętu lub uszkodzenie oprogramowania,
e) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,
f) usiłowanie zakłócenia działania systemu informatycznego.

§ 2

W przypadku stwierdzenia faktu nieprawidłowego przetwarzania, ujawnienia lub nienależytego zabezpieczenia przed osobami nieupoważnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia ochrony danych osobowych, każdy pracownik Ośrodka, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa jest zobowiązany fakt ten niezwłocznie zgłosić ABI. W razie niemożliwości zawiadomienia ABI należy powiadomić osobę przez niego upoważnioną i jednocześnie Kierownika Ośrodka.

§ 3

Do czasu przybycia na miejsce naruszenia ochrony danych osobowych lub danych wrażliwych ABI lub upoważnionej przez niego osoby, należy :

a) Niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyny lub sprawców,
b) Rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
c) Zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,

d) Podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
e) Podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
f) Zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
g) Udokumentować wstępnie zaistniałe naruszenie,
h) Nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby upoważnionej.

§ 4

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych i danych wrażliwych, ABI lub osoba go zastępująca :

a) Zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Ośrodka,
b) Może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
c) Rozważa celowość i potrzebę powiadomienia ADO,
d) Nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami z jednostki nadrzędnej lub pracownikami firm specjalistycznych.

§ 5

ABI dokumentuje zaistniały przypadek naruszenia danych osobowych oraz sporządza raport wg wzoru stanowiącego załącznik nr 14, który powinien zawierać w szczególności :

a) Wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
b) Określenie czasu i miejsca naruszenia,
c) Określenie okoliczności towarzyszących i rodzaju naruszenia,
d) Wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
e) Wstępna ocena przyczyn wystąpienia naruszenia,
f) Ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

§ 6

Raport, którym mowa w § 5, ABI niezwłocznie przekazuje ADO, a w przypadku jego nieobecności osobie uprawnionej.

VI – Szkolenie użytkowników

§ 1

Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

§ 2

Za przeprowadzenie szkolenia oraz jego zorganizowanie odpowiada ABI.

§ 3

Przeszkolenie odbywa się poprzez zapoznanie użytkowników z polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym.

VII – Postanowienia końcowe

§ 1

Użytkownicy są zobowiązani zapoznać się z treścią polityki oraz do jej stosowania przy przetwarzaniu danych osobowych.

§ 2

Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

§ 3

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, można wszcząć postępowanie dyscyplinarne.

§ 4

Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie strat.

§ 5

W sprawach nieuregulowanych w niniejszej polityce mają zastosowanie przepisy ustawy oraz wydane na jej podstawie akty wykonawcze.