ZARZĄDZENIE NR 39 / 2014

Dyrektora
Zespołu Wojewódzkich Przychodni Specjalistycznych
W Katowicach
z dnia 4 listopada 2014 roku

w sprawie: wprowadzenia w Zespole Wojewódzkich Przychodni Specjalistyczych w Katowicach Polityki Bezpieczeństwa

Podstawa prawna

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j) Dz.U.z 2002 r. Nr 101, poz. 926 ze zm) oraz § 3 i 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 (Dz.U. z 2004 r. Nr 100, poz. 1024).

Zarządza się, co następuje:

§ 1

Wprowadzam w Zespole Wojewódzkich Przychodni Specjalistycznych w Katowicach Politykę Bezpieczeństwa, której treść stanowi załącznik nr 1 do zarządzenia.

§ 2

Każdy pracownik, mający dostęp do danych osobowych, jest obowiązany zapoznać się z treścią załącznika nr 1 oraz otrzyma upoważnienie do przetwarzania danych osobowych.

§ 3

Oświadczenie o zapoznaniu się z treścią powyższych załączników zaopatrzone w podpis pracownika i datę, dołącza się do akt osobowych.

§ 4

Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Polityki Bezpieczeństwa oraz stosowania w pracy pod sankcją konsekwencji służbowych przewidzianych prawem.

§ 5

Treśc Polityku Bezpieczeństwa podlega upowszechnieniu poprzez zamieszczenie na stronie internetowej Biuletynu Informacji Publicznej ZWPS w Katowicach.

§ 6

Nadzór nad wprowadzeniem zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 7

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Zespołu Wojewódzkich Przychodni Specjalistycznych
w Katowicach
Grzegorz Nowaczyński

Sprawdzono pod względem merytorycznym (sporządzający)
Administrator Bezpieczeństwa Informacji
Zbigniew Data

Sprawdzono pod względem prawnym
ADWOKAT
Przemysław Gatarz

Sprawdzono pod względem formalnym
Z-ca DYREKTORA
ds. Ekonomiczno-Administracyjnych
Zespołu Wojewódzkich Przychodni Specjalistycznych
w Katowicach
mgr Agnieszka Knapik

ZATWIERDZAM

POLITYKA BEZPIECZEŃSTWA W ZESPOLE WOJEWÓDZKICH PRZYCHODNI SPECJALISTYCZNYCH W KATOWICACH

SPIS TREŚCI:

WSTĘP

1. Postanowienia ogólne

2. Definicje 4

3. Cel 6

4. Zakres stosowania 6

ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych osobowych 7

2. Administrator Bezpieczeństwa Informacji 7

3. Administrator Systemu Informatycznego 9

4. Kierownik Poradni, Pracowni, Działu 9

5. Osoba upoważniona do przetwarzania danych osobowych 9

6. Infrastruktura przetwarzania danych osobowych 10

STRUKTORY ZBIORÓW DANYCH, SPOSÓB PRZEPŁYWU DANYCH, ZAKRES PRZETWARZANIA DANYCH

1. System Finansowo – Księgowy 11

2. System Kadrowy 11

3. System Płacowy - zintegrowany system ewidencyjno-analityczny 11

4. Program fakturowania 11

5. System do rozliczeń z NFZ 12

6. Program do rozliczeń z ZUS 12

Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym

1. Bezpieczeństwo osobowe 14

2. Strefy bezpieczeństwa 15

3. Zabezpieczenie sprzętu 15

4. Zabezpieczenia we własnym zakresie 16

5. Postępowanie z nośnikami i ich bezpieczeństwo 17

6. Wymiana danych i ich bezpieczeństwo 18

7. Kontrola dostępu do systemu 19

8. Kontrola dostępu do sieci 19

9. Komputery przenośne i praca na odległość 19

10. Monitorowanie dostępu do systemu i jego użycia 20

11. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych (art.26ust. ustawy) 20

12. Udostępnianie danych osobowych 21

13. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych 22

14. Przeglądy polityki bezpieczeństwa i kontroli systemu 22

15. Postępowanie w sytuacji naruszenia ochrony danych osobowych 23

16. Postanowienia końcowe 24

1. Postanowienia ogólne

Administrator danych, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń bezpieczeństwa danych osobowych przetwarzanych w związku z wykonywaniem zadań, deklaruje podejmowanie wszelkich możliwych działań koniecznych do minimalizowania ryzyka w celu zapobiegania zagrożeniom, m. in. takim jak:

1. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej i inne;

2. niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych np. nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne;

3. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych i inne o podobnym charakterze;

4. podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;

5. celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora danych;

6. ataki z Internetu;

7. naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do ich przetwarzania, związane z nieprzestrzeganiem procedur w tym zakresie, w tym zwłaszcza:

   - niezgodne z procedurami np. zakończenie pracy lub opuszczenie stanowiska pracy, nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza na portiernię itp.,
   - naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   - ujawnienie osobom nieupoważnionym systemu zabezpieczeń ochrony danych i dokumentów z nim związanych stosowanych u administratora danych,
   - ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych,
   - nie wykonywanie stosownych kopii zapasowych,
   - przetwarzanie danych osobowych w celach prywatnych,

- wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu.

2. Definicje

Ilekroć w polityce bezpieczeństwa jest mowa o:

1. Administratorze Danych – rozumie się przez to administratora danych – ZWPS w Katowicach reprezentowanego przez Dyrektora, decydującego o celach i środkach przetwarzania danych osobowych,,
2. Administratorze Bezpieczeństwa Informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji zwany dalej „ABI".
3. Administratorze Systemu Informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora systemu informacji.
4. Danych osobowych - uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
5. Osobie możliwej do zidentyfikowania - jest osoba, 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, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
6. Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
7. Haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi.
8. Identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
9. Integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
10. Odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    - osoby, której dane dotyczą,
    - osoby upoważnionej do przetwarzania danych,
    - przedstawiciela, o którym mowa w art. 31a ustawy,
    - podmiotu, o którym mowa w art. 31 ustawy,
    - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
11. Osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Dyrektora ZWPS na

piśmie,

12. Poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
13. Przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,
14. Raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
15. Rozliczalność – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
16. Rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U nr 100, poz. 1024),
17. Publicznej sieci telekomunikacyjnej – rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U nr 171, poz. 1800 z póź. zm.),
18. Sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U nr 171, poz. 1800 z póź. zm.),
19. Serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,
20. Systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
21. Teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
22. Ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U z 2002 r. nr 101, poz. 926 z póź. zm.),
23. Uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
24. Użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.
25. przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
26. zabezpieczeniu danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
27. usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
28. zgodzie 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,

29. szyfrowaniu – rozumie się przez to zabezpieczenie danych poprzez uczynienie ich nieczytelnymi bez znajomości właściwego klucza/hasła i programu zawierającego algorytm kryptograficzny pozwalający na odczyt danych tylko osobom znającym klucz/hasło.

Pozostałe definicje wynikają z ustawy.

3. Cel

Wdrożenie polityki bezpieczeństwa u Administratora Danych ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym Administratora Danych i poza nim, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.
W obu zbiorach Administratora Danych przetwarzane są między innymi dane wrażliwe, a system informatyczny Administratora Danych posiada szerokopasmowe połączenie z Internetem, niniejsza Polityka Bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

4. Zakres stosowania

1. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

2. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i pozostałych wykonujących świadczenie w ramach innych umów.

Organizacja przetwarzania danych osobowych

1. Administrator danych osobowych

Administrator danych reprezentowany przez Dyrektora ZWPS realizuje zadania Ustawy w zakresie ochrony danych osobowych, w tym zwłaszcza:

1. podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;

2. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;

3. wyznacza Administratora Bezpieczeństwa Informacji oraz określa zakres jego zadań i czynności;

4. wyznacza Administratora Systemu Informacji oraz określa zakres jego zadań i czynności;

5. wyznacza Administratora Bezpieczeństwa Informacji jako właściwego do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych;

6. zleca Z-cy Dyrektora ds. Ekonomiczno- Administracyjnych by we współpracy z Administratorem Systemu Informacji oraz Administratorem Bezpieczeństwa Informacji zapewnił użytkownikom bezpieczne przetwarzanie danych;

7. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator Bezpieczeństwa Informacji

Administrator Bezpieczeństwa Informacji realizuje zadania wynikające z Ustawy w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych i oraz powierzonych obowiązków w tym zwłaszcza:

1. nadzoruje system informatyczny, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,

2. sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,

3. sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,

4. koordynuje wewnętrzne kontrole przestrzegania przepisów o ochronie danych osobowych,

5. nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,

6. nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,

7. przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z GIODO,

8. na wniosek Kierownika Działu przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych (Załącznik nr 4),

9. nadzoruje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,

10. zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby administratorowi danych,

11. wyrejestrowuje użytkowników na polecenie administratora danych lub kierownika działu kadr,

12. zatwierdza wzory dokumentów (odpowiednie klauzule w dokumentach) dotyczących ochrony danych osobowych, przygotowywane przez komórki organizacyjne w statucie administratora danych,

13. nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych wyznaczonych przez administratora danych do ich prowadzenia,

14. prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,

15. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,

16. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego oraz nadzoruje usunięcie skutków naruszenia,

17. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Administratora Danych o naruszeniu ,

18. prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,

19. sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,

20. nadzoruje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

21. przygotowuje wyciągi z polityki bezpieczeństwa, dostosowane do zakresów obowiązków

osób upoważnianych do przetwarzania danych osobowych,

22. przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych,

23. w porozumieniu z administratorem danych osobowych na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę.

3. Administrator Systemu Informatycznego

Administrator Systemu Informatycznego obsługuje system informatyczny administratora danych oparciu o zakres obowiązków lub umowy.

4. Kierownik Działu Kadr

Kierownik Działu Kadr realizuje przede wszystkim następujące zadania w zakresie ochrony danych osobowych:

1. Kierownik działu kadr występuje z wnioskiem do Administratora Danych o nadanie upoważnienia do przetwarzania danych osobowych,

2. Kierownik działu kadr występuje z wnioskiem do ABI o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych,

3. Kierownik działu kadr występuje do ABI z wnioskiem o odwołanie upoważnienia do przetwarzania danych osobowych i/lub wyrejestrowania użytkownika z systemu informatycznego.

5. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1. może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2. musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych lub świadczenia usługi w oparciu o inna umowę a także po ustaniu stosunku pracy lub innej umowy lub odwołaniu z pełnionej funkcji;

3. zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz

postanowieniami niniejszej polityki i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych(Załącznik nr 3);

4. stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;

5. korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;

6. zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym w sposób wskazany w instrukcji.

6. Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych

Obszar przetwarzania danych osobowych w tym w szczególności budynki i pomieszczenia wchodzące w jego skład zostanie określony zarządzeniem Dyrektora ZWPS (załącznik nr 1).

2. Zbiory danych

Zbiory danych, systemy oraz programy do ich przetwarzania zgodnie z zapisami niniejszej Polityki Bezpieczeństwa, miejsce ich lokalizacji oraz stanowiska odpowiedzialne za poszczególne czynności zostaną określone zarządzeniem Dyrektora ZWPS (załącznik nr 1).

3. System informatyczny

System informatyczny Administratora Danych stanowią między innymi serwery, stacje robocze, łącza, zabezpieczenia, inne urządzenia oraz procedury i instrukcje z nimi związane

4. Ewidencje z zakresu ochrony danych osobowych

W ramach struktury organizacyjnej Administratora Danych prowadzone są następujące ewidencje wchodzące w skład dokumentacji z zakresu ochrony danych osobowych:

1. Administrator Bezpieczeństwa Informacji prowadzi ewidencję udostępnień danych odbiorcom danych oraz innym podmiotom,

2. Administrator Bezpieczeństwa Informacji prowadzi przechowywaną w kasie pancernej ewidencję haseł do stanowisk roboczych poszczególnych użytkowników oraz ich identyfikatorów, a także ewidencje: komputerów przenośnych, nośników przenośnych oraz kluczy kryptograficznych,

3. Administrator Systemu Informatycznego generuje hasła dostępu lub gromadzi hasała dostępu i przekazuje w stosownym terminie administratorowi bezpieczeństwa informacji.

Struktury zbiorów danych, sposób przepływu danych i zakres przetwarzania danych.

1. System Finansowo – Księgowy

Dane dotyczące programu, algorytmów, struktury bazy danych, zgodne z „Ustawą o rachunkowości".

2. System Kadrowy

W zakres programu wchodzi:

- obsługa kartotek kadrowych zawierających dane osobowe i kadrowe zgodnie z obowiązującymi przepisami w tym zakresie.

3. System Płacowy - zintegrowany system ewidencyjno-analityczny

- obsługa kartotek płacowych zawierających podstawowe dane płacowe i podatkowe każdego pracownika oraz comiesięczne naliczenia składników, potrąceń i zasiłków ZUS.
- obsługa kartotek zwolnień chorobowych, zasiłku macierzyńskiego i opieki
- funkcje pozwalające przygotować comiesięczne dane niezbędne do obliczeń płac funkcje obliczania list płac wg algorytmów zgodnych z obowiązującymi przepisami i regulaminem wynagradzania przyjętym dla szpitala
- rozliczenia podatkowe zgodnie z obowiązującymi przepisami
- funkcje wydruków list płac i zestawień zbiorczych

Program zabezpieczony jest przy uruchomieniu hasłem, a pliki bazy danych umieszczone są na serwerze sieciowym, z dostępem po podaniu nazwy użytkownika i hasła logowania.

4. Program fakturowania

W księgowości ZWPS zainstalowany jest program pozwalający wystawiać faktury dla firm i osób. Program umożliwia wystawianie faktur oraz wydruk rejestru i zestawień
W zakres programu wchodzi:

- rejestr faktur
- kartoteki danych klientów
- kartoteki świadczonych usług
- funkcje obsługi i wydruku faktur
- funkcje wydruku rejestrów VAT-owskich
- funkcje wydruków zestawień faktur zapłaconych i niezapłaconych

5. System do rozliczeń z NFZ

Jest to system rejestrujący dane pozwalające na rozliczenie się ZWPS z NFZ. Stanowiska obejmują rejestracje przychodni, statystykę. Poprzez łącze ZWPS i Internet dane są przekazywane do NFZ.

6. Program do rozliczeń z ZUS

Do rejestracji i przesyłania danych związanych z ubezpieczeniami społecznymi ZUS używany jest standardowy program, dostarczany przez ZUS. Przesyłanie danych następuje za pomocą Internetu. Dane przesyłane do ZUS podpisywane są kwalifikowanym podpisem, zgodnie z wymaganiem ZUS.

Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym

Ze względu na fakt, że system informatyczny administratora danych połączony jest z siecią publiczną, należy zapewnić wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym. Wynikające z tego konsekwencje trzeba uwzględnić w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych (Załącznik nr 3).

1. Bezpieczeństwo osobowe

1. Zachowanie poufności

1. Ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.

2. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia administratora danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

2. Szkolenia w zakresie ochrony danych osobowych

1. Administrator Bezpieczeństwa Informacji uwzględnia następujący plan szkoleń:

a. szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,

b. szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,

c. przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

2. Tematyka szkoleń powinna obejmować w szczególności:

a. przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,

b. sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,

c. obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,

d. odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,

e. zasady i procedury określone w polityce bezpieczeństwa.

2. Strefy bezpieczeństwa

W siedzibie administratora danych wydzielono strefę bezpieczeństwa klasy I, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli. W skład tej strefy wchodzą:

1. pomieszczenie z serwerem (serwerownia), w którym mogą przebywać wyłącznie informatycy, inne osoby upoważnione do przetwarzania tylko w towarzystwie tych pracowników, a osoby postronne w ogóle nie mają dostępu; złożony na portierni klucz do tego pokoju jest przechowywany w zaplombowanym woreczku;
2. pomieszczenie księgowości z kasą pancerną (Kasa), w którym mogą przebywać pracownicy księgowości, inni użytkownicy danych tylko w towarzystwie pracowników księgowości, a osoby postronne w ogóle nie mają dostępu.
3. W strefie bezpieczeństwa klasy II do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych.

3. Zabezpieczenie sprzętu

1. Serwer jest zlokalizowany w odrębnym, klimatyzowanym pomieszczeniu, zamykanym. W pokoju tym mogą przebywać wyłącznie informatycy, inne osoby upoważnione do przetwarzania tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu.
2. Informatycy wskazują użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację systemu informatycznego, a zwłaszcza:

- ochronę nośników przenośnych – w tym także nośników danych, na których przechowywane są kopie zapasowe,
- prawidłową lokalizację komputerów.

3. Wszystkie urządzenia systemu informatycznego serwerowni administratora danych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS) a pozostałe w razie konieczności.
4. Okablowanie sieciowe docelowo będzie wykonane w ten sposób, że dostęp do linii teletransmisyjnych będzie możliwy tylko z pomieszczeń zamykanych na klucz. W miarę możliwości będzie zachowana zasada nie krzyżowania się kabli sieciowych z okablowaniem zasilającym, co będzie zapobiegało interferencjom.
5. Bieżąca konserwacja sprzętu wykorzystywanego przez administratora danych do przetwarzania danych prowadzona jest tylko przez jego pracowników, przede wszystkim informatyków. Natomiast naprawy nie możliwe do wykonania przez zatrudnionych Informatyków, wykonywane są przez personel firm zewnętrzny, które realizowane są w siedzibie administratora danych po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.
6. Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania

danych.

Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące, a także przez administratora bezpieczeństwa informacji.

4. Zabezpieczenia we własnym zakresie

Ważne dla bezpieczeństwa danych jest wyrobienie nawyku przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika:

1. ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
2. niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach;
3. dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
4. niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);
5. pilnego strzeżenia akt, dyskietek, pamięci przenośnych i komputerów przenośnych;
6. kasowania po wykorzystaniu danych na dyskach przenośnych;
7. nieużywania powtórnie dokumentów zadrukowanych jednostronnie (danymi osobowymi lub informacjami niejawnymi);
8. niezapisywanego hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
9. powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
10. przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;
11. opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
12. kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki: magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;
13. nie wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
14. wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby

zapobiec ich utracie;

15. kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;
16. niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
17. niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
18. zachowania tajemnicy danych, w tym także wobec najbliższych;
19. chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy. W przypadku pomieszczenia archiwum stosuje się przepisy wewnętrzne;
20. umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
21. zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
22. zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
23. zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza na portierni, oraz zamykania drzwi na klucz w razie opuszczania pomieszczenia bez pozostawiania go w zamku i oddawania na przechowanie.

24. zasady udostępniania i wypożyczanie dokumentacji medycznej, niemedycznej w Archiwum:

- Kierownicy poszczególnych komórek medycznych i niemedycznych wystawiają upoważnienia dla pracowników na udostępnianie i wypożyczanie dokumentacji archiwum, która dotyczy w/w komórek.

- Archiwum udostępnia oraz wypożycza materiały dla osób wyłącznie upoważnionych.

- Wzór Upoważnienia do Udostępniania i Wypożyczania Dokumentacji Medycznej i Niemedycznej w Archiwum określa załącznik nr ... do Polityki Bezpieczeństwa.

5. Postępowanie z nośnikami i ich bezpieczeństwo

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać:

1. dane z nośników przenośnych nie będących w użytkowaniu i nie stanowiących kopii zapasowych po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty DVD, CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;

2. uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w sposób uniemożliwiający odtworzenie zawartości danych pod nadzorem ABI.
3. zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane osobowe lub informacje niejawne. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;
4. po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

6. Wymiana danych i ich bezpieczeństwo

1. Bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach serwera. Pozwala to – przynajmniej w pewnym stopniu – uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego administratora danych.
2. Sporządzanie kopii zapasowych następuje w trybie opisanym w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.
3. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora bezpieczeństwa informacji oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.
4. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.
5. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu w porozumieniu z administratorem bezpieczeństwa informacji. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora bezpieczeństwa informacji lub informatyków oraz umożliwić im monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.
6. Administrator Systemu Informacji w porozumieniu z Administratorem Bezpieczeństwa Informacji dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.
7. Należy stosować następujące sposoby kryptograficznej ochrony danych:
   - przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron https://.

7. Kontrola dostępu do systemu

Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator Bezpieczeństwa Informacji lub z jego upoważnienia inny pracownik po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. W razie potrzeby, Administrator Bezpieczeństwa Informacji lub z jego upoważnienia inny pracownik może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nie posiadającej statusu pracownika.
Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez Administratora Bezpieczeństwa Informacji po odebraniu od osoby upoważnionej do przetwarzania danych oświadczenia zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz potwierdzenie odbioru pierwszego hasła.
Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji i informatyków.

8. Kontrola dostępu do sieci

1. System informatyczny posiada szerokopasmowe połączenie z Internetem. Dostęp do niego jest jednak ograniczony. Na poszczególnych stacjach roboczych można przeglądać tylko wyznaczone strony www związane z zakresem wykonywanych świadczeń.
2. Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.
3. Korzystanie z zasobów planowanej sieci wewnętrznej jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.
4. Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać wyłącznie pracownicy upoważnieni przez Dyrektora ZWPS po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

9. Komputery przenośne i praca na odległość

1. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby administratora danych nie powinny być pozostawiane bez nadzoru w miejscach publicznych.
2. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach.
3. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.
4. Wykorzystywanie komputerów przenośnych administratora danych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez

osoby nieupoważnione.

5. W domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do administratora danych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych.
6. Administrator Systemu Informacji w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady:

- postępowania w razie nieobecności w pracy dłuższej niż 30 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym Administratora Bezpieczeństwa Informacji i uzgodnić z nim zwrot komputera przenośnego administratorowi danych;
- zwrotu sprzętu w razie zakończenia pracy u administratora danych.

7. W zakresie nieuregulowanym w polityce bezpieczeństwa stosuje się do pracy z wykorzystaniem komputerów przenośnych postanowienia Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

10. Monitorowanie dostępu do systemu i jego użycia

Systemy informatyczne będą monitorowane poprzez okresowe kontrole stacji roboczych.

11. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych (art. 26 ust. 1 ustawy)

1. Administrator Bezpieczeństwa Informacji przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza kierownicy poszczególnych działów, są obowiązani współpracować z Administratorem Bezpieczeństwa Informacji w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.
2. Administrator Bezpieczeństwa Informacji może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.
3. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez Administratora Bezpieczeństwa Informacji i Administratora Danych Osobowych (kierownika jednostki), w której usunięto dane osobowe.
4. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, a w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych zgodnie z art. 24 i 25 ustawy.
5. Administrator Bezpieczeństwa Informacji przygotuje wykaz zbiorów danych (ewidencyjnych), w którym poszczególnym kategoriom danych osobowych przypisane

zostaną okresy ich przechowywania. Wykaz ten zostanie sporządzony po przeanalizowaniu przepisów wyznaczających m.in. obowiązek przechowywania dokumentacji czy też okresy przedawnienia roszczeń udokumentowanych z wykorzystaniem danych osobowych. Przed sporządzeniem takiego wykazu przygotowany zostanie wykaz przepisów, na mocy których przetwarzane są dane osobowe, na podstawie wykazów cząstkowych, sporządzonych przez poszczególne komórki organizacyjne.

12. Udostępnianie danych osobowych

Udostępnianie danych osobowych na podstawie ustawy

Udostępnianie danych osobowych odbiorcom danych może nastąpić wyłącznie po złożeniu wypełnionego wniosku, którego wzór został ustalony w załączniku nr 1 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych.

Udostępnianie danych osobowych na podstawie ustaw szczególnych

Udostępnianie informacji Policji

1. Udostępnianie danych osobowych funkcjonariuszom Policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
   - oznaczenie wnioskodawcy,
   - wskazanie przepisów uprawniających do dostępu do informacji,
   - określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
   - wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.
2. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.
3. Osoba udostępniająca dane osobowe jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.
4. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
5. Jeśli policjant pouczył osobę udostępniającą informacje o konieczności zachowania w tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień.

13. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

1. stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,
2. niezabezpieczenia nośnika lub komputera przenośnego,
3. zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych.

14. Przeglądy polityki bezpieczeństwa i kontroli systemu

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych Administrator Bezpieczeństwa Informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb. Administrator Bezpieczeństwa Informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1. zmian w budowie systemu informatycznego,
2. zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
3. zmian w obowiązującym prawie.

Administrator Bezpieczeństwa Informacji lub osoby wyznaczone przez Dyrektora ZWPS i po jego akceptacji mogą, stosownie do potrzeb, przeprowadzić wewnętrzną kontrolę zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie kontroli wymaga uzgodnienia jej zakresu z Administratorem Systemu Informacji. Zakres, przebieg i rezultaty kontroli dokumentowane są na piśmie w protokole podpisywanym przez Administratora Bezpieczeństwa Informacji lub osoby wyznaczone przez Dyrektora ZWPS.
Dyrektor ZWPS, biorąc pod uwagę wnioski Administratora Bezpieczeństwa Informacji lub inne osoby przeprowadzające kontrolę, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

15. Postępowanie w sytuacji naruszenia ochrony danych osobowych

Postępowanie określa Załącznik nr 4 do niniejszego dokumentu - Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

16. Postanowienia końcowe

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie (Załącznik nr 2), potwierdzające znajomość jego treści.

Polityka Bezpieczeństwa wchodzi w życie 4 listopada 2014 r.

Spis załączników

Załącznik nr 1

wykazu pomieszczeń i zakres przetwarzanych w nich danych osobowych w ZWPS

Załącznik nr 2

upoważnienia do przetwarzania danych osobowych

Załącznik nr 3

Instrukcja zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych

Załącznik nr 4

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

Załącznik nr 1

Wykaz pomieszczeń ZWPS – przetwarzanie i dostęp do danych osobowych				
	03	Archiwum		
	05	Archiwum		
	06	Archiwum - Pracownia Badań Przesiewowych		
	07	Archiwum		
	011	Centrala telefoniczna/ Archiwum - Pracownia Patomorfologii		
	015	Archiwum		
	017	Archiwum		
	018	Archiwum		
	019	Archiwum		
	020	Archiwum		
	021	Palarnia		
	022	Poradnia Zapobiegania i Leczenia Uzależnień		
	023	Poradnia Zapobiegania i Leczenia Uzależnień		
	024	Archiwum		
	026	Archiwum		
	027	Archiwum		
	L06	Archiwum		
	L09	Archiwum		
	031	Archiwum		
	032 + 032 A	Poradnia Zapobiegania i Leczenia Uzależnień (2 drzwi do pomieszczenia)		
	033	Archiwum Pracowni Patomorfologii		
	034	Archiwum		
	040	Archiwum		
Parter	2	Poradnia Neurologiczna/ Neurochirurgiczna/ Rehabilitacyjna - Rejestracja		
	2A	Poradnia Rehabilitacyjna		
	3	Poradnia Neurologiczna/ Neurochirurgiczna/ Rehabilitacyjna		
	4	Poradnia Hematologiczna - Rejestracja		
	5	Poradnia Hematologiczna		
	6	Poradnia Hematologiczna		
	7	Poradnia Hematologiczna		
	8	Poradnia Hematologiczna		
	9	Poradnia Hematologiczna		
	10	Poradnia Hematologiczna		
	11	Pracownia RTG		
	12	Pracownia RTG		
	13	Pracownia RTG		
	14	Pracownia RTG		
	15	Pracownia RTG		
	16	Pracownia RTG		
	17	Poradnia Neurologiczna/ Neurochirurgiczna/ Rehabilitacyjna		
	20	Wodolecznictwo		
	23	Poradnia Laryngologiczna dla Dzieci		
	24	Pracownia Badań Przesiewowych		
	26	Poradnie Stomatologiczne - Poradnia Ortodontyczna		

	27	Poradnie Stomatologiczne		
	28	Poradnie Stomatologiczne - Poradnia Stomatologii Dziecięcej		
	30	Poradnie Stomatologiczne - poradnia Stomatologii Zachowawczej		
	31	Poradnie Stomatologiczne - poradnia Stomatologii Zachowawczej		
	32	Poradnie Stomatologiczne - poradnia Stomatologii Zachowawczej		
	33	Poradnie Stomatologiczne - rejestracja		
	Serwerownia	na terenie Centralnego Laboratorium		
I piętro	101	Poradnia - Rejestracja		
	102	Poradnia Ortopedyczna/ Reumatologiczna - zabiegowy		
	103	Poradnia Ortopedyczna/ Reumatologiczna		
	104	Poradnia Ortopedyczna/ Reumatologiczna		
	105	Poradnia Ortopedyczna/ Reumatologiczna		
	106	Pracownia Rehabilitacji Leczniczej - Sala gimnastyczna		
	107	Pracownia Rehabilitacji Leczniczej		
	108	Pracownia Rehabilitacji Leczniczej		
	109	Pracownia Rehabilitacji Leczniczej		
	110	Pracownia Rehabilitacji Leczniczej		
	111	Pracownia Patomorfologii		
	112	Poradnia Foniatryczna		
	113	Poradnia Foniatryczna		
	114	Pracownia Rehabilitacji Leczniczej - WC		
	118	Poradnia Ortopedyczna - Gipsownia		
	119	Rejestracja Poradni		
	120	Poradnia Kardiologiczna dla Dzieci - Pracownia UKG		
	121	Poradnia Kardiologiczna dla Dziec - Pracownia EKG		
	122	Poradnia Hematologiczna dla Dzieci/ Kardiologiczna dla Dzieci		
	123	Poradnia Hematologiczna dla Dzieci/ Kardiologiczna dla Dzieci		
	124	Poradnia Hematologiczna dla Dzieci/ Kardiologiczna dla Dzieci - rejestracja		
	125	Poradnia Kardiologiczna dla Dzieci		
	126	Pracownia EEG		
	127	Poradnia Reumatologiczna dla Dzieci/ Poradnia Gastroenterologiczna dla Dzie4ci		
	128	Pracownia Rehabilitacji Leczniczej dla Dzieci- Sala gimnastyczna		
	130	Poradnia Neurologiczna dla Dzieci/ Poradnia Rehabilitacyjna dla Dzieci/ Poradnia Wad Rozwojowych		
	131	Poradnia Endokrynologiczna dla Dzieci		
	132	Poradnia Chorób Metabolicznych/ Poradnia Gastroenterelogiczna dla Dzieci		
	Rejestracja Poradnia Alergologiczna			
	1			
	2			
	Zabiegowy Poradni Alergologicznej			
	3			

	4			
	4 A			
	5			
	119	Poradnia Chorób Płuc i Gruźlicy		
	120	Poradnia Chorób Płuc i Gruźlicy		
	121	Poradnia Chorób Płuc i Gruźlicy		
	122	Poradnia Chorób Płuc i Gruźlicy		
	123	Poradnia Chorób Płuc i Gruźlicy		
	124	Poradnia Chorób Płuc i Gruźlicy		
	125	Poradnia Chorób Płuc i Gruźlicy		
	126	Poradnia Chorób Płuc i Gruźlicy		
	127	Poradnia Chorób Płuc i Gruźlicy		
	128			
	129	Poradnia Chorób Płuc i Gruźlicy dla Dzieci i Młodzieży		
	129 A	Poradnia Chorób Płuc i Gruźlicy dla Dzieci i Młodzieży		
	129 B	Poradnia Chorób Płuc i Gruźlicy dla Dzieci i Młodzieży		
II piętro	201	Poradla Leczenia Bólu		
	202	Poradnia Leczenia Bólu		
	203	Poradnia Leczenia Bólu dla Dzieci		
	204	Poradnia Okulistyczna		
	205	Poradnia Okulistyczna		
	205 A	Poradnia Okulistyczna		
	206	Poradnia Okulistyczna		
	206 A	Poradnia Okulistyczna		
	206 B	Poradnia Okulistyczna		
	207	Poradnia Okulistyczna		
	208	Poradnia Okulistyczna		
	209	Poradnia Okulistyczna		
	210	Poradnia Okulistyczna		
	211	Poradnia Okulistyczna		
	212	Poradnia Okulistyczna		
	215	Poradnia Okulistyczna		
	216	Poradnia Okulistyczna		
	218	Poradnia Nefrologiczna		
	219	Poradnia Nefrologiczna		
	220	Poradnia Skórno-Wenerologiczna - zabiegowy		
	221	Poradnia Skórno-Wenerologiczna		
	222	Poradnia Skórno-Wenerologiczna - Rejestracja		
	223	Poradnia Skórno-Wenerologiczna		
	224	Poradnia Skórno-Wenerologiczna		
	225	Poradnia Skórno-Wenerologiczna		
	226	Poradnia Skórno-Wenerologiczna		
	227	Poradnia Skórno-Wenerologiczna		
	228	Poradnia Skórno-Wenerologiczna		
	229	Poradnia Zdrowia Psychicznego		
	230	Poradnia Zdrowia Psychicznego		
	231	Poradnia Zdrowia Psychicznego		
	233	Poradnia Zdrowia Psychicznego		
	234	Poradnia Zdrowia Psychicznego		
	235	Poradnia Zdrowia Psychicznego		

	236	Poradnia Zdrowia Psychicznego		
	237	Poradnia Zdrowia Psychicznego		
	238	Poradnia Zdrowia Psychicznego - Rejestracja		
	239	Poradnia Zdrowia Psychicznego		
	240	Poradnia Zdrowia Psychicznego		
	241	Poradnia Zdrowia Psychicznego		
	242	Poradnia Zdrowia Psychicznego		
	243	Poradnia Zdrowia Psychicznego		
	245	Poradnia Okulistyczna dla Dzieci		
	247	Poradnia Alergologiczna dla Dzieci/ Poradnia Szczepień		
	248	Poradnia Dermatologiczna dla Dzieci/ Poradnia Endokrynologiczna dla Dzieci		
	249	Pracownia Techniki Dentystycznej/ Pracownia Ortodontyczna		
	250	Pracownia Techniki Dentystycznej/ Pracownia Ortodontyczna		
	251	Poradnia Alergologiczna dla Dzieci		
	252	Poradnia Alergologiczna dla Dzieci - Zabiegowy		
	254	Poradnia Ginekologii Dziecięcej/ Leczenia Niepłodności - Gabinet lekarski		
	255	Poradnia Ginekologii Dziecięcej/ Leczenia Niepłodności - Gabinet lekarski		
	256	Poradnia Ginekologii Dziecięcej/ Leczenia Niepłodności - Gabinet położnej		
	257	Poradnia Ginekologii Dziecięcej/ Leczenia Niepłodności - Gabinet USG		
	259	Poradnia Dermatologiczna dla Dzieci/ Poradnia Hepatologiczna		
	260	Poradnia Alergologiczna dla Dzieci/ Dermatologiczna dla Dzieci/ Okulistyczma dla Dzieci/ Szczepień - Rejestracja		
	301	Poradnia Kardiologiczna - Pracownia EKG		
	302	Poradnia Kardiologiczna - Pracownia EKG		
	303	Poradnia Chorób Naczyń		
	306	Pracownia USG		
	307	Pracownia USG		
	308	Poradnia Endokrynologiczna		
	309 A	Poradnia Endokrynologiczna		
	310	Poradnia Endokrynologiczna		
	311	Poradnia Endokrynologiczna		
	312	Poradnia Endokrynologiczna		
	313	Poradnia Endokrynologiczna		
	314	Gabinet Badań Profilaktycznych		
	315	Naczelna Pielęgniarka		
	316	Dział Płac		
	317	Dział Księgowości		
	318	Główna Księgowa		
	319	Z-ca Dyrektora		
	320	Radca Prawny		
	321	Kierownik działu Kadr		
	322	Dział Kadr		
	323	Sekretariat		
	325	Dział Administracyjno-Techniczny		

	326	Dział Lecznictwa		
	327	Dział Lecznictwa		
	327 A	Z-ca Dyrektora		
	336	Poradnia Endokrynologiczna		
	337	Poradnia Endokrynologiczna		
	340	Poradnia Kardiologiczna		
	341	Poradnia Chorób Naczyń		
	342	Wejście na strych		
	343	Poradnia Medycyny Sportowej, Poradnia Nefrologiczna dla Dzieci		
	344	Poradnia Kardiologiczna		
	345	Poradnia Kardiologiczna		
	355	Poradnia Kardiologiczna		
	356	Poradnia Kardiologiczna		
	360	Poradnia Medycyny Sportowej, Poradnia Nefrologiczna dla Dzieci		
IV piętro	401	Dział Administracyjno-Techniczny - Informatycy		

Załącznik nr 2 Katowice .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Upoważniam Panią/Pana.....

Zatrudnioną/zatrudnionego w Zespole Wojewódzkich Przychodni Specjalistycznych w Katowicach ul. Powstańców 31
do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków służbowych na stanowisku

[ ] lekarz [ ] pracownik biurowy [ ] rejestratorka medyczna

[ ] pielęgniarka [ ] położna [ ] technik medyczny

[ ] psycholog [ ] inne

oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład. Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.) i elektronicznej.

Upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w zbiorach na stanowisku pracy.

[ ] KS-SOMED - program do obsługi poradni [ ] Patomorfolog

[ ] KS-SOLAB - program do obsługi laboratorium

[ ] Program KADRY [ ] Program Płace [ ] Program Płatnik

[ ] Program Finansowo-Księgowy

[ ] Programy dedykowane do Poradni Okulistycznej [ ] Programy dedykowane do Poradni Kardiologicznej

[ ] Programy dedykowane do Poradni Chorób Płuc [ ] Programy dedykowane do Pracowni EEG

[ ] Programy dedykowane do Poradni Zdrowia Psychicznego [ ] Programy dedykowane do Poradni Alergologicznej

Inne a) .....

b).....

.....
(podpis i pieczęć ABI)

Osoba upoważniona do przetwarzania danych jest zobowiązana do:

1) Zapoznania się i wypełniania obowiązków wynikających z przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz przepisów wykonawczych wydanych na jej podstawie,

2) Zachowania w tajemnicy danych oraz informacji o ich zabezpieczeniu, również po ustaniu zatrudnienia.

3) Zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.

.....
(podpis osoby upoważnionej)

Załącznik nr 4

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

1. Niniejsza instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych zarówno w postaci papierowej jak i przetwarzanych w Systemie Informatycznym ZWPS w Katowicach. Instrukcję stosuje się w przypadku stwierdzenia naruszenia zabezpieczeń sprzętu informatycznego, sieci komputerowej lub zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.

2. Każda osoba przetwarzająca dane osobowe w ZWPS, która stwierdzi lub podejrzewa naruszenie ochrony danych w wersji papierowej lub w Systemie Informatycznym, zobowiązana jest do niezwłocznego poinformowania o tym Administratora Bezpieczeństwa lub w przypadku jego nieobecności bezpośredniego przełożonego.

3. Do czasu przybycia Administratora Bezpieczeństwa na miejsce naruszenia ochrony danych osobowych, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze 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, 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 Administratora Bezpieczeństwa.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy ZWPS,
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3) jeżeli zasoby systemu na to pozwalają, generuje i drukuje wszystkie raporty, które mogą pomoc w ustaleniu wszelkich okoliczności zdarzenia,
   4) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych:
      a) fizycznie odłącza urządzenia i segmenty sieci, które mogłyby umożliwić dostęp do bazy danych osobie niepowołanej,

b) wylogowuje użytkownika podejrzanego o naruszenie ochrony danych,
c) zmienia hasła konta administratora i użytkownika, poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.

5) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora Danych Osobowych,
6) jeżeli zachodzi taka potrzeba, nawiązuje kontakt ze specjalistami spoza ZWPS.

5. Po wyczerpaniu niezbędnych środków doraźnych, Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze oraz ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii bezpieczeństwa i terminu wznowienia przetwarzania danych.
6. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   2) określenie czasu i miejsca naruszenia i powiadomienia,
   3) określenie okoliczności towarzyszących i rodzaju naruszenia,
   4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   5) wstępną ocenę przyczyn wystąpienia naruszenia,
   6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
7. Raport, o którym mowa w ust. 6 Administrator Bezpieczeństwa przekazuje Administratorowi Danych Osobowych w terminie 14 dni od daty zdarzenia.
8. Wzór raportu, o którym mowa w ust. 6 i 7 jest określony w końcowej części niniejszej instrukcji.
9. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Wzór raportu z naruszenia bezpieczeństwa
Systemu w ZWPS w Katowicach

1. Data: ..... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko służbowe, identyfikator użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

.....

5. Podjęte działania:

.....

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....

.....
(podpis Administratora Bezpieczeństwa)