Powiatowa Stacja
Sanitarno-Epidemiologiczna
09-300 Żuromin, ul. Przemysłowa 10
tel. /23/ 657 22 17, tel./fax /23/ 657 38 88
Kod PKD 8412Z
NIP 511-000-35-80, Regon 130288316

ZARZĄDZENIE Nr 5/2018

DYREKTORA POWIATOWEJ STACJI SANITARNO-EPIDEMIOLOGICZNEJ W ŻUROMINIE

z dnia 25 maja 2018 r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych Powiatowej Stacji Sanitarno-Epidemiologicznej w Żurominie

Na podstawie art. 10 ust. 4 ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (Dz.U. z 2017 r. poz. 1261 z późn. zm.) oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) zarządzam, co następuje:

§ 1.

Wprowadza się w Powiatowej Stacji Sanitarno-Epidemiologicznej w Żurominie **Politykę ochrony danych osobowych**, stanowiącą załącznik Nr 1 do zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

§ 3.

Traci moc Zarządzenie Nr 12/2011 z dnia 31 października 2011 r.

DYREKTOR
Powiatowej Stacji
Sanitarno-Epidemiologicznej w Żurominie
mgr Agnieszka Cyran

RADCA PRAWNY
Jarosław Miński
nr wpisu OL 915

Załącznik Nr 1 do Zarządzenia
Nr 5/2018
Dyrektora PSSE w Żurominie
z dnia 25 maja 2018 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

Powiatowej Stacji Sanitarno-Epidemiologicznej

w Żurominie

Spis treści:

Strona nr

Załączniki:

- załącznik nr 1 - Wzór upoważnienia do przetwarzania danych osobowych
- załącznik nr 2 - Wzór oświadczenia o poufności i zapoznaniu się z przepisami
- załącznik nr 3 - Polityka czystego biurka
- załącznik nr 4 - wzór Rejestru Czynności Przetwarzania Danych
- załącznik nr 5 - wzór Rejestru Kategorii Czynności Przetwarzania
- załącznik nr 6 - wzór Rejestru Naruszeń Ochrony Danych

I. Podstawa prawna:

1. Niniejszy dokument zatytułowany **„Polityka ochrony danych osobowych"** (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Powiatowej Stacji Sanitarno -Epidemiologicznej w Żurominie (dalej jako **PSSE**).

   Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1). (dalej jako **RODO**).

2. Polityka zawiera:

   1) opis zasad ochrony danych obowiązujących w PSSE;

   2) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);

3. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Administrator Danych Osobowych.

4. Za monitorowanie przestrzegania Polityki odpowiada Inspektor Ochrony Danych Osobowych.

5. Za stosowanie niniejszej Polityki odpowiedzialni są wszyscy członkowie personelu PSSE. PSSE zapewnia możliwość zaznajomienia się z niniejszą Polityką podmiotom przetwarzającym dane osobowe na mocy umów powierzenia zawartych z PSSE.

6. PSSE zapewnia zgodność przetwarzania danych osobowych z regulacjami RODO oraz krajowymi przepisami dotyczącymi ochrony danych osobowych - szczególnie w odniesieniu do: petentów i pracowników PSSE, a ponadto danych osobowych powierzonych do przetwarzania podmiotom trzecim.

II. Podstawowe pojęcia i skróty:

1) **Polityka** - oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
2) **RODO** - oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).
3) **Dane** - oznaczają dane osobowe, wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, o ile co innego nie wynika wyraźnie z kontekstu.
4) **Dane wrażliwe** - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej
5) **Dane szczególne** - oznaczają dane specjalne karne oraz dane dzieci.
6) **Dane karne** - oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
7) **Dane dzieci** - oznaczają dane osób poniżej 16. roku życia.
8) **Osoba** - oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
9) **Podmiot przetwarzający** - oznacza organizację lub osobę, której PSSE powierzyła przetwarzanie danych osobowych.
10) **Eksport danych** - oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
11) **IODO lub Inspektor** - oznacza Inspektora Ochrony Danych Osobowych
12) **RCPD lub Rejestr** - oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
13) **RNOD** - oznacza Rejestr Naruszeń Ochrony Danych,
14) **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

15) **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

16) **Administrator Danych Osobowych (ADO)** – Dyrektor Powiatowej Stacji Sanitarno -Epidemiologicznej w Żurominie;

III. Cele i zasady bezpieczeństwa ochrony danych osobowych:

1. **Filary ochrony danych osobowych w PSSE:**
   1) **Legalność** – PSSE dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
   2) **Bezpieczeństwo** – PSSE zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
   3) **Prawa osób** – PSSE umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
   4) **Rozliczalność** – PSSE dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

2. **Zasady ochrony danych**

   PSSE działa w oparciu o podstawę prawną - ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (Dz.U. z 2017 r. poz. 1261 z późń. zm.) i zgodnie z prawem (legalizm);
   1) rzetelnie i uczciwie (rzetelność);
   2) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
   3) w konkretnych celach i nie "na zapas" (minimalizacja);
   4) nie więcej niż potrzeba (adekwatność);
   5) z dbałością o prawidłowość danych (prawidłowość);
   6) nie dłużej niż potrzeba (czasowość);
   7) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

3. **System ochrony danych**

   System ochrony danych osobowych w PSSE składa się z następujących elementów:

   1) **Inwentaryzacja danych. Ocena skutków dla ochrony danych.** PSSE w terminie co najmniej do końca stycznia danego roku kalendarzowego (lub każdorazowo w trakcie

roku kalendarzowego - jak dodawane (odejmowane) są kolejne kategorie przetwarzanych danych) dokonuje identyfikacji zasobów przetwarzanych danych osobowych, kategorii danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

a) przypadków przetwarzania danych wrażliwych,

b) przypadków przetwarzania danych osób, których PSSE nie identyfikuje (**dane niezidentyfikowane**);

c) współadministrowania danymi.

2) **Rejestr.** PSSE opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych oraz Rejestr Kategorii Czynności Przetwarzania. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w PSSE.

3) **Umowy powierzenia przetwarzania danych.** PSSE zawiera z podmiotami lub osobami, którym powierza przetwarzanie danych osobowych (np. usługodawca - informatyk, podmiot wykonujący usługi opiekuńcze, podmiot realizujący pomoc rzeczową na rzecz beneficjentów PSSE) odpowiednie umowy, stosownie do art. 28 RODO.

4) **Podstawy prawne.** PSSE zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy PSSE przetwarza dane na podstawie prawnie uzasadnionego interesu PSSE

5) **Obsługa praw jednostki.** PSSE spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a) **Obowiązki informacyjne.** PSSE przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

b) **Możliwość wykonania żądań.** PSSE weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

c) **Obsługa żądań. PSSE** zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.

d) **Zawiadamianie o naruszeniach.** PSSE stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony

danych.

6) **Minimalizacja.** PSSE posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

a) zasady zarządzania **adekwatnością** danych;

b) zasady reglamentacji i zarządzania **dostępem** do danych;

c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

7) **Bezpieczeństwo.** PSSE zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

c) dostosowuje środki ochrony danych do ustalonego ryzyka;

d) posiada system zarządzania bezpieczeństwem informacji; (w tym systemem informatycznym)

e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami. PSSE opracowuje, prowadzi i utrzymuje Rejestr Naruszeń Ochrony Danych Osobowych w PSSE. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w PSSE.

f) wydaje upoważnienia do przetwarzania danych osobowych dla pracowników i innych osób wykonujących czynności przetwarzania danych tj. stażyści, praktykanci. Określa w upoważnieniu wyraźny zakres przetwarzania danych osobowych. **Wzór upoważnienia stanowi załącznik nr 1 do Polityki.**

g) wydaje oświadczenia o poufności i zapoznaniu się z przepisami. **Wzór oświadczenia stanowi załącznik nr 2 do Polityki.**

8) ***Privacy by design.*** PSSE zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów lub zadań PSSE uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

IV. Zabezpieczenia danych osobowych:

1. Ochrona zbiorów danych polega na zabezpieczeniu informacji wprowadzonej,

przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem.

2. W celu ochrony danych przechowywanych w systemach informatycznych należy wykorzystywać wchodzące w ich skład mechanizmy zarówno sprzętowe jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo danych.

3. Dane osobowe mogą przetwarzać wyłącznie osoby posiadające upoważnienia do przetwarzania danych osobowych. Osoby upoważnione do przetwarzania danych mają obowiązek zachować w tajemnicy dane, które przetwarzają, oraz sposoby ich zabezpieczenia.

4. Fakt modyfikacji zbioru danych: struktury, lokalizacji, a także utworzenia nowego zbioru osoba upoważniona, która takiej modyfikacji dokonała ma obowiązek zgłosić ten fakt ADO.

5. Osoby nieupoważnione do przetwarzania danych osobowych mogą przebywać w obszarach przetwarzania danych osobowych jedynie za zgodą ADO lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

6. Wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych - także w godzinach pracy.

7. Klucze do pomieszczeń służbowych mogą pobierać tylko te osoby, które są umieszczone w „wykazie osób upoważnionych do pobierania kluczy" po dokonaniu podpisu w „księdze pobierania i zdawania kluczy od pomieszczeń służbowych"

8. Dane osobowe przechowywane w wersji tradycyjnej (papierowej) są przechowywane po zakończeniu pracy w zamykanych na klucz meblach biurowych, a tam gdzie jest to możliwe - w szafach metalowych lub pancernych. Klucze od szaf należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych.

9. Dokumenty zawierające dane osobowe, w wyjątkowych sytuacjach mogą być wynoszone poza miejsce przetwarzania jedynie w wypadku otrzymania akredytacji ADO z jednoczesnym zapewnieniem ochrony fizycznej ich przed niepożądanym dostępem osób nieupoważnionych. Odpowiedzialność za dokumentację ponosi pracownik, który otrzymał akredytację.

10. Po zakończonej pracy klucze do pomieszczeń, w których przetwarza się dane osobowe, oddaje się upoważnionemu pracownikowi, który zabezpiecza je przed nieuprawnionym dostępem w odpowiednim miejscu do tego wyznaczonym. Fakt

przyjęcia kluczy pracownik odnotowuje w odpowiedniej ewidencji.

11. Dane osobowe w wersji papierowej, wydruki i kopie a także, w wersji elektronicznej na nośnikach typu płyty CD, DVD, dyskach przenośnych należy niszczyć w niszczarkach lub przekazywać do zniszczenia wynajętej do tego celu firmie. Dokumentacja niszczona w niszczarkach poddawana jest całkowitej utylizacji.

12. Sprzątanie pomieszczeń gdzie przetwarzane są dane osobowe odbywa się po godzinach pracy przez personel sprzątający, który został upoważniony imiennie do przebywania w pomieszczeniach przetwarzania danych osobowych. Sprzątanie odbywa się tylko z założeniem, że zostaną zachowane przez pracowników przetwarzających dane osobowe zasady „czystego biurka i ekranu".

13. Przy przetwarzaniu danych osobowych w systemach teleinformatycznych stosuje się zasady „czystego biurka i ekranu", realizowane poprzez stosowanie wygaszacza ekranu, blokowania systemu za pomocą indywidualnych haseł lub kodów oraz ustawianie monitorów w taki sposób aby nie była widoczna informacja dla osób postronnych. **„Polityka czystego biurka" stanowi załącznik nr 3 do Polityki.**

14. Zabrania się udostępniania indywidualnego kodu dostępu i haseł innym osobom.

15. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki.

16. Zabrania się korzystania z prywatnych nośników informacji w systemach przetwarzających dane osobowe.

17. Zabrania się korzystania z sieci publicznej (World Wide Web) poprzez nieautoryzowane przeglądarki internetowe lub nieznajomego pochodzenia witryny internetowe.

18. W przypadku żądania udostępniania danych pracownicy PSSE postępują zgodnie z przepisami dotyczącymi ochrony danych osobowych. Decyzję podejmuje ADO w porozumieniu z IODO.

19. Udostępnianie danych jest odnotowywane w systemach informatycznych, a w przypadku zbiorów danych w formie tradycyjnej odnotowanie informacji o udostępnianiu przechowuje ADO.

20. Dla danych osobowych przetwarzanych w systemach informatycznych stosuje się następujące zasady:

a. kontrola dostępu do zbiorów danych osobowych;

b. indywidualne identyfikatory użytkowników (pracowników przetwarzających dane osobowe);

c. uwierzytelnianie użytkowników (potwierdzanie ich tożsamości).

21. W celu zabezpieczenia danych osobowych przed ich utratą lub uszkodzeniem:

a) dla wszystkich systemów wdrożono procedury tworzenia kopii zapasowych;

b) wszystkie systemy informatyczne wyposażono w awaryjne zasilanie;

c) wdrożono oprogramowanie antywirusowe;

d) dostęp do systemów z sieci publicznej jest kontrolowany za pomocą zapory sieciowej oraz filtrów antyspamowych i oprogramowania antywirusowego;

e) przy przesyłaniu danych osobowych przez sieć publiczną użytkownicy są zobowiązani stosować oprogramowanie szyfrujące;

f) zastosowano środki fizyczne chroniące urządzenia przed osobami nieupoważnionymi przez ADO do dostępu do danych osobowych oraz zagrożeniami ze strony sił natury.

22. Użytkowników systemów przetwarzających dane osobowe obowiązuje następująca polityka haseł:

a) minimalna długość hasła wynosi 8 (osiem) znaków;

b) zmiana hasła następuje nie rzadziej, niż co 30 dni;

c) hasło może się powtórzyć dopiero po 6 zmianie;

d) hasło zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;

e) hasła zgłaszane są do osoby upoważnionej przez ADO, która zabezpiecza rejestry haseł dla danego użytkownika komputera.

23. Jeżeli system informatyczny środkami technicznymi nie wymusza zasad ujętych powyżej, użytkownik zobowiązany jest do przestrzegania powyższych zasad, a tym samym do okresowej zmiany hasła i dobrania odpowiedniej jego długości.

24. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie ADO, który ustali nowe hasło.

25. Zabezpieczanie danych przed ich utratą uszkodzeniem, lub nieupoważnionym przetworzeniem w pozostałych przypadkach:

a) W przypadku naprawy, przekazania, likwidacji nośnika (papier, dysk twardy, płyta kompaktowa, pamięć przenośna, dyskietka, taśma magnetyczna itp.), który zawiera dane osobowe podmiotowi nieupoważnionemu do przetwarzania danych, należy zapewnić trwałe wymazanie informacji stanowiących dane osobowe, z wyłączeniem sytuacji, kiedy naprawy, przekazania, likwidacji nośnika dokonuje podmiot z którym ADO w tym zakresie zawarł umowę powierzenia;

b) W przypadku korzystania z komputerów przenośnych zawierających dane osobowe należy zachować szczególną ostrożność podczas używania komputera poza obszarem przetwarzania danych. W szczególności należy stosować mechanizmy szyfrowania

plików lub baz danych, wbudowanych w system operacyjny. Po ustaniu konieczności przetwarzania danych na komputerze przenośnym, należy je trwale usunąć z nośnika danych;

c) Ekrany komputerów, na których przetwarzane są dane osobowe, są chronione wygaszaczami. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych;

d) W pomieszczeniach gdzie przetwarzane dane osobowe są szczególnie narażone na ich przetworzenie przez osoby nieuprawnione stosuje się zabezpieczenia fizyczne w postaci odgrodzenia stref przetwarzania danych osobowych poprzez montaż np.: i. przezroczystych szyb, drzwi; ii. drewnianych półek, lad, blatów. Powyższe odgrodzenia mają na celu zabezpieczenie strefy szczególnie narażonych na przetwarzanie danych osobowych przed nieuprawnionym dostępem do strefy więcej niż jednej osoby bez wiedzy upoważnionego pracownika do przetwarzania danych osobowych, w pomieszczeniach gdzie zachowanie zasady „czystego biurka" jest ze względów logistycznych, fizycznych (brak miejsca) nie jest możliwe do zrealizowania. Wstęp do strefy przetwarzania danych osobowych następuje za zgodą upoważnionego pracownika.

V. Rejestry:

1. Rejestr Czynności Przetwarzania Danych (RCPD)

1) RCPD stanowi formę dokumentowania czynności przetwarzania danych osobowych w PSSE. RCPD pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2) PSSE prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

3) RCPD jest jednym z podstawowych narzędzi umożliwiających PSSE rozliczanie większości obowiązków ochrony danych.

4) W RCPD, dla każdej czynności przetwarzania danych, którą PSSE uznała za odrębną dla potrzeb RCPD, PSSE odnotowuje co najmniej:

a) nazwę czynności,

b) cel przetwarzania,

c) opis kategorii osób,

d) opis kategorii danych,

e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu PSSE, jeśli podstawą jest uzasadniony interes,

f) sposób zbierania danych,

g) opis kategorii odbiorców danych (w tym przetwarzających),

h) informację o przekazaniu poza EU/EOG;

i) ogólny opis technicznych i organizacyjnych środków ochrony danych.

5) Wzór RCPD stanowi **Załącznik nr 4 do Polityki - "Wzór Rejestru Czynności Przetwarzania Danych".** Wzór Rejestru zawiera także kolumny nieobowiązkowe.

W kolumnach nieobowiązkowych PSSE rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść RCPD ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej. Rejestr sporządzony jest w formie elektronicznej pliku XLS.

2. Rejestr Kategorii Czynności Przetwarzania (RKCP)

1) RKCP stanowi formę dokumentowania czynności przetwarzania danych osobowych w PSSE jako przetwarzający w imieniu innego Administratora Danych. RKCP pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2) PSSE prowadzi RKCP, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

3) RKCP jest jednym z podstawowych narzędzi umożliwiających PSSE rozliczanie większości obowiązków ochrony danych.

4) W RKCP, dla każdej czynności przetwarzania danych, którą PSSE uznała za odrębną dla potrzeb RKCP, PSSE odnotowuje co najmniej:

a) Kategorie przetwarzań,

b) Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,

c) Nazwa i dane kontaktowe administratora,

d) dane inspektora ochrony danych administratora,

e) informacje czy dane są przekazywane do państwa trzeciego i organizacji międzynarodowej.

5) Wzór RCPD stanowi **Załącznik nr 5 do Polityki - "Wzór Rejestru Kategorii**

Czynności Przetwarzania". Wzór Rejestru zawiera także kolumny nieobowiązkowe.

W kolumnach nieobowiązkowych PSSE rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść RKCP ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej. Rejestr sporządzony jest w formie elektronicznej pliku XLS.

3. **Rejestr Naruszeń Ochrony Danych (RNOD)**

1) RNOD stanowi formę dokumentowania naruszeń ochrony danych osobowych w PSSE. RNOD pełni rolę sprawdzenia naruszeń oraz środków zaradczych, naprawczych, które w związku z tym wdraża PSSE, a także jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2) PSSE prowadzi RNOD, w którym gromadzi i monitoruje naruszenia ochrony danych osobowych.

3) RNOD jest jednym z podstawowych narzędzi umożliwiających PSSE rozliczanie obowiązku monitorowania naruszeń ochrony danych i stosowania działań zaradczych.

4) W RNOD, dla każdego naruszenia ochrony danych, PSSE odnotowuje co najmniej:

a) naruszenie,

b) Data i godzina zgłoszenia podejrzenia naruszenia,

c) Data oraz godzina stwierdzenia naruszenia,

d) Data naruszenia/okres, którego dotyczy,

e) Kategoria i ilość osób, których dotyczy naruszenie,

f) Miejsce naruszenia,

g) Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia,

h) Opis skutków/konsekwencji naruszenia

i) Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki zastosowane w celu zminimalizowania jego negatywnych skutków,

j) Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych,

k) Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy.

5) Wzór RNOD stanowi **Załącznik nr 6 do Polityki - "Wzór Rejestru Naruszeń Ochrony Danych".** Wzór Rejestru zawiera także kolumny nieobowiązkowe.

W kolumnach nieobowiązkowych PSSE rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść RNOD ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej. Rejestr sporządzony jest w formie elektronicznej pliku XLS.

4. **Podstawy przetwarzania**

1) PSSE dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

2) Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel PSSE) PSSE dookreśla podstawę w czytelny sposób, gdy jest to potrzebne.

3) PSSE wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

4) Kierownik komórki organizacyjnej PSSE ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes PSSE, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes PSSE.

VI. Zgłaszanie naruszeń:

1. **Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu**

1) W przypadku naruszenia w PSSE ochrony danych osobowych, kierownik/dyrektor PSSE bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2) Zgłoszenie naruszenia w PSSE ochrony danych osobowych musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez PSSE w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

2. **Zawiadamianie o naruszeniu ochrony danych osobowych osoby, której naruszenie dotyczy**

1) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, PSSE bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2) Zawiadomienie musi być sporządzone jasnym i prostym językiem, opisywać charakter naruszenia ochrony danych osobowych oraz zawierać co najmniej

a) informacje o IODO,

b) konsekwencjach naruszenia,

c) środkach zaradczych.

3) PSSE zwolniony jest z obowiązku zawiadomienia osoby jeśli:

a) wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,

b) zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby,

c) wymagałoby ono niewspółmiernie dużego wysiłku.

VII. Inspektor Ochrony Danych Osobowych:

1. **Wyznaczenie Inspektora Ochrony Danych**

1) Status prawny i zadania Inspektora ochrony danych regulują przepisy Rozdziału IV Sekcji 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

2) Inspektor ochrony danych w wykonywaniu swoich zadań podlega bezpośrednio kierownikowi/dyrektorowi PSSE.

3) Do zadań Inspektora ochrony danych należy w szczególności:

a) informowanie Dyrektora oraz pracowników PSSE, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach;

b) monitorowanie przestrzegania rozporządzenia RODO, innych przepisów dotyczących ochrony danych osobowych oraz prowadzenie szkoleń wewnętrznych zwiększających świadomość personelu PSSE w zakresie zasad dotyczących ochrony danych,

c) pełnienie funkcji punktu kontaktowego dla właściwych organów i podmiotów zewnętrznych w kwestiach związanych z przetwarzaniem przez PSSE danych osobowych.

4) IODO nie rzadziej niż raz na kwartał przeprowadza audyt wewnętrzny stosowania dokumentacji ochrony danych osobowych oraz rozwiązań technicznych i organizacyjnych w PSSE.

5) Z audytu o którym mowa w pkt. 4 IODO sporządza protokół, określający zakres kontroli, stan stosowania regulacji ochrony danych osobowych, a także zalecenia co do dalszego przetwarzania.

VIII. Postanowienia końcowe:

1. W sprawach nieobjętych niniejszym dokumentem mają zastosowanie odpowiednie przepisy prawa w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. , poz. 1000).
2. Każda osoba upoważniona do przetwarzania danych osobowych w PSSE jest obowiązana do zapoznania się oraz stosowania postanowień Polityki.
3. Polityka wchodzi w życie z dniem ogłoszenia
4. Z dniem wejścia w życie Polityki traci moc .**Polityka bezpieczeństwa danych osobowych** wprowadzona zarządzeniem z dnia 31.10.2011 r.

DYREKTOR
Powiatowej Stacji
Sanitarno-Epidemiologicznej w Żurominie
mgr Agnieszka Cyran

Załącznik nr 1 do Polityki Ochrony Danych Osobowych

....., dn. ..... 20..... r.

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych .....

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Kodeksu pracy, a także z Polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych.

Okres ważności
od:
do:

.....
podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia .....

Odwołano, dnia .....

.....
podpis osoby uprawnionej do odwołania upoważnienia

Załącznik nr 2 do Polityki Ochrony Danych Osobowych

Oświadczenie

o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany(a) ....., stanowisko .....

..... oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem:

Rodzaj zadań	*)
zadań i obowiązków służbowych wynikających z umowy o pracę	
zadań wynikających z umowy cywilno-prawnej	
zadań wynikających z umowy – w związku z praktyką studencką	
zadań wynikających z umowy o zorganizowanie stażu	

*) właściwe zaznaczyć X

zarówno w trakcie wykonywania umowy jak i po jej ustaniu.

Zobowiązuję się przestrzegać dokumentów wewnętrznych ochrony danych osobowych. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych. Zobowiązuję się do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przez niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskiwaniem. Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących zasadach, dotyczących przetwarzania danych osobowych określonych w „Polityce Ochrony Danych Osobowych".

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy z dnia 10.05.2018r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000) oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

Oświadczam że zostałem(am) poinformowany o grożącej odpowiedzialności karnej i cywilnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

....

/ miejscowość i data złożenia oświadczenia/ /czytelny podpis osoby składającej oświadczenie/

Załącznik nr 3 do Polityki Ochrony Danych Osobowych

POLITYKA CZYSTEGO BIURKA
w Powiatowej Stacji Sanitarno-Epidemiologicznej w Żurominie

1. Niniejsza polityka czystego biurka obowiązuje wszystkich pracowników zatrudnionych w Powiatowej Stacji Sanitarno-Epidemiologicznej w Żurominie.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, doktoranta, studenta i ucznia, niebędący pracownikami, oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.
3. Za pracodawcę uważa się Powiatową Stację Sanitarno-Epidemiologiczną w Żurominie.
4. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
5. Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu.
6. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy.
7. Po zakończonej pracy pracownik zobowiązany jest odłożyć laptopa do zamykanej na klucz szafy.
8. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.
9. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.

Załącznik nr 4 do Polityki Ochrony Danych Osobowych

Rejestr czynności przetwarzania

Nazwa i dane kontaktowe administratora	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

Załącznik nr 5 do Polityki Ochrony Danych Osobowych

Rejestr kategorii czynności przetwarzania

Nazwa i dane kontaktowe przetwarzającego	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

Rejestr Naruszeń Ochrony Danych Powiatowej Stacji Sanitarno-

L.p.	Naruszenie (stypizowany opis naruszenia)	Data i godzina zgłoszenia podejrzenia naruszenia
1.		
2.		

Epidemiologicznej w Żurominie

Data oraz godzina stwierdzenia naruszenia	Data naruszenia/okres, którego dotyczy

[redacted]

Kategoria i ilość osób, których dotyczy naruszenie

[redacted]

Zakres danych i/lub kategorie danych, których dotyczy naruszenie

[redacted]	
Osoba/źródło informacji o zdarzeniu	**Miejsce naruszenia**

[redacted]

Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia

Opis skutków/konsekwencji naruszenia	**Osoba/jednostka odpowiedzialna za naruszenie**

[redacted]

Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki zastosowane w celu zminimalizowania jego negatywnych skutków

Rezultat działań naprawczych	**Osoba odpowiedzialna za wdrożenie działań naprawczych**

[redacted]

Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych (Jeśli tak - data i godzina zgłoszenia; w przypadku wystąpienia opóźnienia w powiadomieniu - wyjasnienie przyczyn opóźnienia)

[redacted]

Czy poinformowano organy ścigania (data zawiadomienia)

[redacted]

Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy oraz sposób przekazania informacji wraz opisem zaleceń dla podmiotów danych

Monitoring działań naprawczych