POLITYKA OCHRONY DANYCH OSOBOWYCH

CENTUM USŁUG WSPÓLNYCH OŚWIATY

Spis treści

I. WSTĘP

1. Informacje ogólne

Celem Polityki Bezpieczeństwa Ochrony Danych Osobowych, zwanej dalej Polityką, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Centrum Usług Wspólnych Oświaty (CUWO) grupy informacji zawierającej dane osobowe.

Opisane i zastosowane w niej zabezpieczenia mają zapewnić:

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

2. Cel przygotowania polityki bezpieczeństwa

Podstawowym celem przygotowania i wdrożenia dokumentu jest zapewnienie zgodności działania Centrum Usług Wspólnych Oświaty w Radomiu z Rozporządzeniem 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) oraz polskim regulacjom prawnym.

3. Zakres informacji objętych polityką bezpieczeństwa oraz zakres stosowania

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zbiór działań zmierzających do uzyskania i utrzymania wymaganego poziomu bezpieczeństwa danych osobowych, tj. zapewnienie poufności, spójności i dostępności na każdym etapie tworzenia, przetwarzania, przechowywania i przesyłania danych osobowych.

Polityka Bezpieczeństwa, odnosi się całościowo do problemu zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie, jak i w systemach informatycznych (w odniesieniu, do których w przypadku szczegółowych regulacji występuje odesłanie do procedur).

Jako załącznik do niniejszej polityki opracowano i wdrożono procedury. Określają one sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, oraz danych osobowych poza systemem informatycznym ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

II. Definicje

Administrator danych osobowych (ADO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. Tożsamość tej osoby fizycznej.

Dane genetyczne – oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

Dane biometryczne – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

Dane dotyczące zdrowia – oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – ujawniające informacje o stanie jej zdrowia;

Szczególne kategorie danych osobowych – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Przetwarzanie danych osobowych – dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania – polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Dokumentacja medyczna – chronologicznie uporządkowany zbiór danych dotyczących stanu zdrowia i choroby pacjenta oraz udzielonych mu świadczeń zdrowotnych.

Anonimizacja – zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.

Zgoda osoby, której dane dotyczą – oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych – to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób

fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (**Procesor)** – osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Inspektor Ochrony Danych (IOD) – osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi / Podmiotowi przetwarzającemu / pracownikom w zakresie obowiązującego prawa o ochronie danych niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Pseudonimizacja – oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szczególne kategorie danych osobowych – ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Naruszenie ochrony danych osobowych – jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych

Państwo trzecie – państwo nie należące do Europejskiego Obszaru Gospodarczego.

Pracownik – osoba pozostająca z ADO w związku na podstawie umowy o pracę lub umowy cywilnoprawnej.

Polityka Ochrony Danych Osobowych – niniejszy dokument.

Administrator Systemu Informatycznego (ASI) – to osoba formalnie wyznaczona przez ADO w celu nadzorowania sprawności systemu informatycznego oraz w celu informowania i doradzania w związku z zapewnieniem właściwej ochrony systemu informatycznego, szczególnie w celu ochrony danych osobowych.

Konto zwykłe – konto, którego użytkownik posiada dostęp jedynie do niezbędnych danych umożliwiających wykonywanie powierzonych mu obowiązków służbowych.

Konto uprzywilejowane – konto, którego użytkownik posiada szeroki dostęp do infrastruktury IT oraz do krytycznych zasobów (tj.: serwery, rutery, macierze, bazy danych, systemy plików, materiały stanowiące

własność intelektualną chronioną prawami autorskimi, kody źródłowe, ważne i poufne dane, systemy dostępu, itp.).

III. ODPOWIEDZIALNOŚĆ W ZAKRESIE ZARZĄDZANIA BEZPIECZEŃSTWEM

1. Deklaracja

ADO, mając świadomość, że przetwarza dane osobowe, w tym dane osobowe pracowników, deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa oraz stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

2. ADO - zadania i obowiązki

1. ADO obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
2. realizuje obowiązek informacyjny wobec osoby, której dane dotyczą oraz przestrzega praw osoby, której dane dotyczą, m. in. prawa do dostępu oraz zapomnienia;
3. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
4. powołuje IOD;
5. wyznacza ASI;
6. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych;
7. zapewnia przetwarzanie danych zgodnie z uregulowaniami Polityki Bezpieczeństwa Informacji, sprawuje nadzór nad bezpieczeństwem danych osobowych.

3. IOD – zadania i obowiązki:

1. informowanie ADO, podmiotów przetwarzających oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych wymagań prawnych;
2. monitorowanie przestrzegania RODO, innych wymagań prawnych dotyczących ochrony danych osobowych oraz Polityki, w tym podział obowiązków, działania zwiększające świadomość, szkolenia pracowników uczestniczących w operacjach przetwarzania oraz powiązane z tym audyty;
3. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania;
4. współpraca z organem nadzorczym;
5. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z konsultacjami związanymi oceną skutków dla ochrony danych oraz we wszelakich innych sprawach;

6. pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO;
7. prowadzenie rejestru czynności przetwarzania.

4. ASI – zadania i obowiązki:

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1. Formułuje, w uzgodnieniu z administratorem danych lub osobami, którym ADO delegował zarządzanie uprawnieniami oraz IOD, sposobu określania uprawnień w systemach informatycznych.
2. Realizowanie decyzji ADO odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT CUWO tj.:
    1. tworzenie kont użytkowników w systemach informatycznych,
    2. resetowanie utraconych haseł,
    3. usuwanie kont i uprawnień dla kont osób, które zakończyły pracę w CUWO,
    4. dostarczanie ADO lub IOD informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowo-programowych.
3. Planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w CUWO.
4. Planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych.
5. Automatyzacja zadań konserwacyjnych w systemie – w tym wykonywania kopii zapasowych oprogramowania i danych.
6. Monitorowanie stanu środowiska IT, stanu sprzętu i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników.
7. Monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych.
8. Zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych.
9. Systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego.
10. Zapewnienie eksploatowanym systemom opieki serwisowej producenta – zawieranie umów regulujących formy tej opieki.
11. Rozwiązywanie, samodzielnie i we współpracy z pozostałym personelem IT, problemów towarzyszących eksploatacji systemów informatycznych.
12. Przygotowywanie, we współpracy z IOD instrukcji dla użytkowników systemów informatycznych.

5. Osoba upoważniona do przetwarzania danych

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 bądź 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, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.
3. Musi zapoznać się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki Bezpieczeństwa.
4. Stosuje określone przez Administratora Danych oraz Inspektora Ochrony Danych procedury oraz wytyczne mające na celu przetwarzanie danych osobowych zgodnie z obowiązującym prawem.
5. Korzysta z systemu informatycznego Administratora Danych w sposób zgodny z procedurami.
6. Zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. PRZETWARZANIE DANYCH OSOBOWYCH

1. Pomieszczenia w których przetwarza się dane osobowe

1. Pomieszczeniami tworzącymi obszar, w którym znajdują się przetwarzane dane osobowe są pomieszczenia, w których znajdują się zbiory danych w formie kartotek, rejestrów i innej oraz stacjonarny sprzęt komputerowy, w którym są przetwarzane dane osobowe.
2. Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania, osób nieuprawnionych do dostępu do danych osobowych, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.
3. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane i chronione na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osób trzecich.

V. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI PRZETWARZANYCH DANYCH

W Placówce rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   - pomieszczenia zamykane na klucz,
   - szafy zamykane na klucz,
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   - przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   - przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia organizacyjne:
   - osobą odpowiedzialną za bezpieczeństwo danych jest IOD,
   - ASI na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami. IOD kontroluje sposób, systematyczność oraz prowadzoną dokumentację z zakresu kontroli.
4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:

- w CUWO jest stworzony rejestr osób upoważnionych, który na bieżąco jest aktualizowany,
- przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie,
- w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
- przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,
- w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
- po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

VI. KONTROLA WEWNĘTRZNA STANU OCHRONY DANYCH OSOBOWYCH I PRZESTRZEGANIA ZASAD ICH OCHRONY

1. IOD sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych.
   1.1. IOD lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
   1.2. W szczególny sposób nadzorowany jest całościowo System Zabezpieczenia Przetwarzania Danych Osobowych.
      1.2.1. Przegląd Systemu Zabezpieczeń odbywa się nie rzadziej niż raz do roku.
      1.2.2. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
         1.2.2.1. procesów funkcjonujących w strukturach Administratora Danych,
         1.2.2.2. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
2. IOD sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Realizuje to za pomocą audytów.
   2.1. IOD przeprowadza audyt według opracowanego planu audytów.
   2.2. IOD przygotowuje plan audytów na okres nie krótszy niż kwartał i nie dłuższy niż rok z zaznaczeniem, że plan musi obejmować co najmniej jeden audyt.
   2.3. Plan audytów IOD przygotowuje w formie papierowej bądź elektronicznej i przedstawia Administratorowi Danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
   2.4. W planie audytów IOD uwzględnia, w szczególności:
      2.4.1. przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,
      2.4.2. procesy przetwarzania danych osobowych objęte audytem,
      2.4.3. konieczność weryfikacji zgodności przetwarzania danych osobowych z:
         2.4.3.1. zasadami przetwarzania danych osobowych,
         2.4.3.2. zasadami dotyczącymi zabezpieczenia danych osobowych,
         2.4.3.3. zasadami przekazywania danych osobowych.
   2.5. W toku audytu IOD dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
   2.6. Po zakończeniu audytu, IOD przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
   2.7. IOD przekazuje Administratorowi Danych sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.
3. Raz w roku Inspektor Danych Osobowych przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych.

4. Zaobserwowane błędy oraz zaniechania w przestrzeganiu Polityki oraz całości Systemu przedstawia się ADO oraz pracownikom upoważnionym do przetwarzania danych osobowych.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, IOD dokonuje aktualizacji Polityki w wymaganym zakresie.

VII. SZKOLENIA LUB ZAPOZNAWANIE OSÓB Z ZASADAMI OCHRONY DANYCH

Każda osoba przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami w wersji papierowej winna być poddana przeszkoleniu lub zapoznana z:

- podstawami prawnymi dotyczącymi bezpieczeństwa danych osobowych,
- zasadami ochrony danych osobowych zawartymi w Polityce,
- procedurami związanymi z ochroną bezpieczeństwa właściwymi dla obejmowanego stanowiska.

2. Za przeprowadzenie szkolenia lub zapoznania z zasadami ochrony danych osobowych odpowiada IOD.
3. Za przeprowadzenie szkolenia lub zapoznania z procedurami właściwymi dla stanowisk odpowiada przełożony nowozatrudnionej osoby.
4. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą listy obecności z przeprowadzonego szkolenia.
5. Każda nowozatrudniona osoba po odbytym szkoleniu lub po zapoznaniu z zasadami ochrony danych osobowych zobowiązana jest do podpisania Zobowiązania do zachowania poufności oraz nadawane jest upoważnienie do przetwarzania danych osobowych..
6. Podpisane Zobowiązania i upoważnienia zostają zarchiwizowane w aktach osobowych lub teczkach pracowników.

VIII. POSTANOWIENIA KOŃCOWE

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody ADO.
2. Polityka Bezpieczeństwa może być udostępniania osobom i instytucjom postronnym bez zgody ADO, jeżeli nie zawiera w treści informacji o zabezpieczeniach danych osobowych, a wszelkie załączniki występują w formie niewypełnionych szablonów.
3. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszej Polityce.
4. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
5. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy Rozporządzenie 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) oraz wydanych na jej podstawie aktów wykonawczych.
6. Zmiana dokonana w załączniku do niniejszej Polityki powoduje aktualizację danego załącznika, nie powoduje natomiast zmiany całości dokumentu. Po dokonaniu aktualizacji załącznika jego wcześniejsza wersja automatycznie traci ważność.

IX. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Instrukcja Zarządzania Systemem Informatycznym została opracowana zgodnie z Rozporządzeniem 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).

Instrukcja stanowi zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych

1. Zabezpieczenia fizyczne

1. zabezpieczono dostęp do kluczowej infrastruktury w postaci budynków, pomieszczeń biurowych, archiwów i miejsc przechowywania kopii bezpieczeństwa,
2. wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej,
3. rozmieszczenie komputerów, drukarek, kopiarek ogranicza dostęp osób nieupoważnionych,
4. dostęp do pomieszczeń zabezpieczono drzwiami zamykanymi na klucz,
5. dostęp do archiwum zabezpieczono drzwiami zamykanymi na klucz,
6. dostęp do dokumentacji i danych w pomieszczeniach zabezpieczono w zamkniętych szafach,

2. Zabezpieczenia techniczne oraz infrastruktury informatycznej i telekomunikacyjnej

1. Wyposażenie jest obsługiwane przez przeszkolony i upoważniony do tego personel.
2. Każdy element wyposażenia jest jednoznacznie etykietowany, oznakowany lub zidentyfikowany w inny sposób.
3. Wyposażenie komputerowe jest przechowywane i eksploatowane w warunkach zapewniających jego prawidłowe funkcjonowanie, zgodnie z wytycznymi producentów.
4. Urządzenia poddaje się kontroli z częstotliwością wynikającą z ich rodzaju i wskazań wytwórców.
5. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane, w tym dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
6. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
7. Wszystkie komputery i laptopy działające w systemie informatycznym posiadają zainstalowane oprogramowanie antywirusowe, dodatkowo sprzęt posiadający połączenie z Internetem chroniony jest zaporą sieciową.
8. Pomieszczenia, w których przechowywany jest sprzęt komputerowy i nośniki informacji są zabezpieczone przed dostępem osób postronnych.

9. Wyposażenie komputerowe zabezpieczone jest przed utratą danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie listwy antyprzepięciowej.
10. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane.

3. Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe

Opis technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych.

1. Dostęp do zbioru danych osobowych (do bazy danych i do programu) wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
3. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
4. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych.
5. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

X. PROCEDURY

- 1 Procedura postępowania z incydentami ochrony danych osobowych
- 2 Procedura oceny skutków dla ochrony danych osobowych
- 3 Procedura realizacji praw osób, których dane dotyczą
- 4 Zasady i sposób odnotowywania informacji o udostępnieniu danych osobowych
- 5 Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych
- 6 Procedura kontroli podmiotów przetwarzających
- 7 Procedura nadawania uprawnień
- 8 Metody i środki uwierzytelniania
- 9 Procedury na stanowisku pracy
- 10 Procedury tworzenia kopii zapasowych
- 11 Zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania
- 12 Procedury wykonywania przeglądów i konserwacji systemów oraz nośników
- 13 Zabezpieczenie i dostęp do infrastruktury
- 14 Postępowanie z nośnikami
- 15 Administrowanie i monitoring systemów informatycznych

XI. Załączniki

- 1 Ocena ryzyka
- 2 Rejestr czynności przetwarzania
- 3 Rejestr kategorii czynności przetwarzania
- 4 Rejestr udostępnień
- 5 Rejestr naruszeń ochrony
- 6 Ewidencja osób upoważnionych do przetwarzania
- 7 Rejestr wykaz budynków
- 8 Wyznaczenie i odwołanie IOD
- 9 Wyznaczenie i odwołanie ASI
- 10 Sprawozdanie z audytu zgodności przetwarzania danych osobowych
- 11 Zgłoszenie naruszenia ochrony danych osobowych
- 12 Protokół naruszenia zasad ochrony danych
- 13 Umowa powierzenia danych
- 14 Porozumienie w zakresie przetwarzania danych osobowych
- 15 Polityka prywatności www
- 16 Zgoda na przetwarzanie danych osobowych pracownika
- 17 Zgoda na przetwarzanie danych osobowych pacjenta
- 18 Klauzula informacyjna do monitoringu z procedurą aplikacji
- 19 Klauzula informacyjna dla pracownika z procedurą aplikacji
- 20 Klauzula informacyjna na www z procedurą aplikacji
- 21 Klauzula informacyjna w procesie rekrutacji z procedurą aplikacji
- 22 Klauzula informacyjna przy stanowisku rejestracji z procedurą aplikacji
- 23 Pracownika oświadczenie o poufności