RODO

POLITYKA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH

LABIRYNT
PIOTR ZWIERZCHOWSKI
UL.WEOSŁA 4 05 816 MICHALOWICE
NIP 113-012 -78-28

I. WPROWADZENIE

1.Niniejszy dokument stanowi politykę bezpieczeństwa i ochrony danych osobowych w jednostce, zwany dalej Polityką. Reguluje całościowo dopuszczalny przez prawo sposób zarządzania i ochrony danych osobowych oraz prawa osób, których dane osobowe są przez jednostkę przetwarzane.

2.Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – 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)

3.Celem Polityki, jest wskazanie działań, jakie należy podjąć, formy tych działań, oraz sposób ich przeprowadzania, aby wykonać ciążące na administratorze danych osobowych obowiązki.

4.Polityka zawiera :

a/. opis zasad ochrony danych osobowych w jednostce

b/. opis środków organizacyjnych i technicznych zapewniający ochronę danych osobowych

c/. określają zasady dostępu, przetwarzania i udostępniania danych osobowych

d/.określenie ryzyka w obszarach bezpieczeństwa fizycznego, informatycznego, osobowego oraz organizacyjno – prawnego

e/. wzorce postępowań

f/. wzorce dokumentów związanych z wypełnieniem obowiązujących norm

SKRÓTY I DEFINICJE

1. Polityka - oznacza niniejszą Politykę ochrony danych osobowych

2. RODO - oznacza 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

3. Dane - oznaczają dane osobowe

4. Dane dzieci - oznaczają dane osób poniżej 16 roku życia

5. Dane wrażliwe - oznaczają dane dotyczące zdrowia

6. Pacjent - oznacza osobę której dane dotyczą a która korzysta ze świadczeń leczniczych w jednostce

7. Osoba - oznacza osobę której dane dotyczą

8. Podmiot przetwarzający - oznacza organizację , podmiot lub osobę której jednostka powierzyła przetwarzanie danych osobowych

9. Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych , które polegają na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osób fizycznych w szczególności do analizy prognozy aspektów dotyczących zdrowia, efektów pracy, sytuacji ekonomicznej.

10. IOD lub INSPEKTOR - oznacza Inspektora Ochrony Danych Osobowych

11. RCPD lub Rejestr - oznacza Rejestr Czynności Przetwarzania Danych Osobowych

12. Jednostka oznacza : podmiot który przetwarza dane osobowe

13. Dokumentacja medyczna - oznacza dokumentację medyczną w rozumieniu ustawy z dnia 6 listopada 2008 r. O prawach pacjenta i Rzeczniku Praw Pacjenta oraz aktów wykonawczych.

14. Opiekun faktyczny - oznacza opiekuna faktycznego w rozumieniu ustawy o Prawach pacjenta i Rzeczniku Praw Pacjent

15. Przedstawiciel ustawowy - osoba umocowana do działania w cudzym imieniu na podstawie art. 96 k.c.

II.ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

A/.ZASADY OGÓLNE

1. Filarami ochrony danych osobowych w jednostce są : legalność, bezpieczeństwo, prawa jednostki, rozliczalność.

2. Legalność jednostka realizuje poprzez dbałość o ochronę prywatności i przetwarza dane zgodnie z prawem

3. Bezpieczeństwo jednostka zapewnia odpowiedni poziom bezpieczeństwa danych.

4. Prawa Jednostki czyli umożliwienie osobom, których dane są przetwarzane przez jednostkę wykonywanie swoich praw i prawa te realizuje.

5. Rozliczalność wykonuje jednostka poprzez dokumentowanie sposobu spełnienia obowiązków związanych z ochroną danych w taki sposób by w każdej chwili móc wykazać zgodność z przepisami.

6. Jednostka przetwarza dane osobowe z poszanowaniem następujących zasad :

A. Legalizm- w oparciu o podstawę prawną i zgodnie z prawem

B. Rzetelność - rzetelnie i uczciwie

C. Transparentność - w sposób przejrzysty dla osoby , której dotyczą

D. Minimalizacja - w konkretnych uzasadnionych celach

E. Adekwatność - nie więcej niż potrzeba

F. Prawidłowość - z dbałością o prawidłowość danych

G. Czasowość - nie dłużej niż wynika to z potrzeb i przepisów

H. Bezpieczeństwo - zapewniając odpowiednie bezpieczeństwo danych

7. System ochrony danych osobowych w jednostce składa się następujących elementów :

A. Inwentaryzacja danych - jednostka identyfikuje zasoby danych osobowych w tym dane wrażliwe, dane dzieci, profilowanie.

B. RCDO - jednostka opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w jednostce.

C. Podstawy prawne - jednostka zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze.

D. Obsługa praw jednostki - jednostka spełnia obowiązki informacyjne względem osób , których dane przetwarza oraz zapewnia obsługę ich praw, realizując w tym zakresie żądania , w tym :

- Obowiązki informacyjne - jednostka przekazuje osobom prawem wymagane informacje i zapewnia udokumentowanie realizacji tych obowiązków

- Możliwość wykonywania żądań - jednostka weryfikuje i zapewnia możliwość wykonania żądania przez siebie i swoich przetwarzających

- Obsługa żądań - jednostka zapewnia odpowiednie procedury aby żądania osób były realizowane w terminach i sposób wymagany RODO i właściwie to dokumentuje

- Zawiadamianie o naruszeniach - jednostka stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

8. Minimalizacja . Jednostka posiada zasady i metody zarządzania minimalizacją w tym zasady zarządzania adekwatnością danych, reglamentacji dostępu do danych, przechowywania danych i weryfikacji dalszej ich przydatności.

9. Bezpieczeństwo jednostka zapewnia poprzez odpowiedni poziom bezpieczeństwa danych w tym przeprowadza analizy ryzyka dla czynności przetwarzania danych, analizę ryzyka kategorii danych, ocenę skutków dla wysokiego ryzyka naruszenia praw, dostosowuje środki ochrony danych do ustalonego ryzyka, posiada procedury zarządzania incydentami.

10. Przetwarzający . Jednostka posiada zasady doboru przetwarzających dane na rzecz jednostki, opracowane zostały zasady przetwarzania (umowy powierzenia) oraz zasady weryfikacji wykonywania umów powierzenia.

11. Jednostka zarządza zmianami wpływającymi na prywatność (Privacy by design).

III. PODSTAWY PRZETWARZANIA DANYCH

1. Jednostka dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności i kręgu osób których dotyczy przetwarzanie.

2. Podstawą przetwarzania danych w jednostce w zależności od kategorii danych jest :

Źródło danych osobowych	Zakres	Podstawa prawna	Cel
UCZEŃ	Dane osobowe zgodne z przepisami, (rejestracja)	UMOWA	Identyfi
Uczeń	Dane kontaktowe telefon, e-mail	UMOWA	Możliwo realizac
Uczeń	Publikacja wizerunku	Pisemna zgoda	Promoc
Podmiot przetwarzający	Dane kontakowe telefon , e-mail	Umowa	Możliwo podmio zamówi

3.

4. Przetwarzanie danych na podstawie zgody pacjenta występuje w sytuacji :

A/. Zgody na wykorzystanie wizerunku dla celów promocji - załącznik nr. 1 do polityki

IV. SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

1. Jednostka dba o czytelność i styl przekazywanych informacji i komunikacji z osobami których dane przetwarza.

2. Jednostka ułatwia korzystanie z ich praw poprzez :

- Umieszczenie w rejestracji jednostki informacji dostępnej o prawach oraz sposobach korzystania z nich :Wzór - załącznik. nr. 2

- Informowanie pisemne o prawach i obowiązkach- Wzór - załącznik. nr. 3

A/. OBOWIĄZKI INFORMACYJNE

1. Jednostka określiła zgodne z prawem i efektywne sposoby wykonania obowiązków informacyjnych.

2. Jednostka informuje osobę o :

- Przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania osoby
- Przetwarzaniu jej danych osobowych przy pozyskaniu danych od tej osoby
- O ograniczeniu przetwarzania
- O sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych
- O prawie sprzeciwu względem przetwarzania danych
- O naruszeniu ochrony danych osobowych gdy może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby
- O tym , że nie przetwarza danych jej dotyczących, jeżeli osoba taka zgłosiła żądanie dotyczące jej praw
- Informacji w ciągu miesiąca od otrzymania żądania o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych
- Na żądanie osoby dot. Dostępu do jej danych jednostka informuje osobę :

• Czy przetwarza jej dane,

• Podaje szczegóły przetwarzania zgodnie z art. 15 RODO - wzór - informacja o zakresie przetwarzania danych załącznik 4

B/.ŻĄDANIA OSÓB

1.Jednostka udziela dostępu do danych poprzez wydanie kopii danych i nie uzna tego za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych

2. Na żądanie wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych

3. Jednostka dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Nadto na żądanie tej osoby informuje o odbiorcach danych.

4. Jednostka uzupełnia i aktualizuje dane na żądanie osoby. Jednostka może odmówić uzupełnienia danych gdyby było to niezgodne z prawdą lub oświadczenie osoby byłoby niewiarygodne.

5. Jednostka dokonuje ograniczenia przetwarzania danych na żądanie osoby gdy :

- osoba kwestionuje ich prawidłowość - na czas pozwalający sprawdzić ich poprawność

- Przetwarzanie jest niezgodne z prawem

- Osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją - do czasu sprawdzenia czy jednostka niema uzasadnionych prawnie nadrzędnych podstaw do nieuwzględnienia sprzeciwu

C/.ZASADA MINIMALIZACJI

1. Jednostka przetwarza dane respektując zasadę minimalizacji przetwarzania danych pod kątem adekwatności do celów, zakresu ich przetwarzania , dostępu do danych oraz czasu ich przechowywania .

2. W celu zachowania zasady minimalizacji jednostka ogranicza dane osobowe ze względu na kategorie osób, cel i czas przetwarzania :

Osoba	Cel	Dane	Okres przetwarzania / przechowywania
Uczeń	Wykonanie umowy	• Imię i nazwisko • Adres zamieszkania • Telefon • E-mail	1 rok

3. Jednostka wprowadza ograniczenia dostępności danych z uwagi na zakresy upoważnień i kręgu osób na powierzone zadania mają dostęp do danych ;

- właściciel w zakresie wykonania umowy

- Księgowy - w zakresie wystawiania rachunków/ faktur

V.ŚRODKI BEZPIECZEŃSTWA

1. Jednostka stosuje środki bezpieczeństwa wynikające z analizy ryzyka i adekwatności środków oraz oceny skutków dla ochrony danych.

2. W jednostce dane podlegają przetwarzaniu :

Zakres przetwarzania	Miejsce
Dane osobowe ucznia	Dokumentacja papierowa

1.W związku z tym, że system informatyczny posiada szerokopasmowe połączenie z Internetem, niniejsza polityka służy zapewnieniu wysokiego poziomu bezpieczeństwa danych. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

2.Celem wdrożonego systemu zarządzania bezpieczeństwem informacji jest osiągnięcie poziomu organizacyjnego i technicznego, który:

- zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych oraz jawnych,

- zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,

- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualne wykorzystanie na szkodę jednostki,

- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,

3.Powyższe cele realizowane są poprzez:

- określeniu zasad przetwarzania informacji, czyli korzysta się z e-maila ucznia w zakresie udzielenia informacji na temat procesu edukacyjnego

- przegląd i aktualizację polityk i procedur postępowania dokonywaną przez odpowiedzialne osoby, w celu jak najlepszej reakcji na zagrożenia i incydenty,

4.Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych, wydane przez ADO

5.Każda osoba upoważniona podpisuje oświadczenie o zachowaniu poufności przetwarzanych danych.

6.Upoważnioną do przetwarzania danych może być tylko osoba, która uczestniczyła uprzednio szkoleniu z zakresu ochrony danych osobowych.

7.Osoba posiadająca upoważnienie do przetwarzania danych jest uprawniona do ich przetwarzania w zakresie i czasie wskazanym w upoważnieniu.

8.Wzór upoważnienia do przetwarzania danych stanowi Załącznik nr 13 do niniejszej Polityki.

9.Wzór oświadczenia o zachowaniu poufności przetwarzanych danych stanowi Załącznik nr 5 do niniejszej Polityki.

VI. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1.Każdy użytkownik odpowiada za ochronę informacji przetwarzanych w systemie zgodnie z indywidualnym zakresem obowiązków, nadanymi uprawnieniami i zakresem odpowiedzialności wynikającym z zajmowanego stanowiska.

2.Obowiązkiem każdego użytkownika jest:

- przestrzeganie przepisów prawa i przepisów wewnętrznych jednostki

- dbałość o zachowanie bezpieczeństwa informacji, do których ma dostęp,

- zgłaszanie do bezpośredniego przełożonego oraz ADO przypadków naruszenia bezpieczeństwa informacji .

4. Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych.

5. ADO odpowiada w szczególności za:

- dokonywanie przeglądu dokumentacji bezpieczeństwa, a w szczególności polityk bezpieczeństwa i procedur, nie rzadziej niż raz w roku.

- dokonywanie bieżącej kontroli nad przestrzeganiem zasad przetwarzania danych. Kontrola polega w szczególności na sprawdzeniu:

- którzy pracownicy mają dostęp do danych osobowych,

- czy dane osobowe nie zostały udostępnione nieupoważnionym pracownikom,

- czy pracownicy i inne osoby mające dostęp do danych osobowych posiadają aktualne upoważnienia do przetwarzania danych osobowych wydane przez ADO.

- monitorowanie zagrożeń, na jakie narażone są zasoby informacyjne ,

- dokonywanie przeglądu i monitorowanie naruszeń bezpieczeństwa informacji.

- nadzór nad przestrzeganiem zasad określonych w polityce i regulacjach wewnętrznych dotyczących ochrony danych osobowych;

- zarządzanie dostępem.

- obowiązany jest każdorazowo sporządzić raport w przypadku naruszenia bezpieczeństwa systemu informatycznego

6. ADO odpowiada za:

- monitorowanie zagrożeń, na jakie narażone są zasoby informatyczne ,

- dokonywanie przeglądu i monitorowanie naruszeń bezpieczeństwa informatycznego,

- bieżącą kontrolę zgodności funkcjonowania z wymaganiami bezpieczeństwa wynikającymi z dokumentacji bezpieczeństwa zasobów informatycznych.

- utrzymanie systemów informatycznych,

- wycofanie systemów informatycznych

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

a. Może przetwarzać dane osobowe zgodnie z zakresem opisanym w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków.

b. Ustanie stosunku pracy powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

c. Musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.

d. Zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki

e. Stosuje określone przez ADO procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne i celowe przetwarzanie danych.

f. Zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

8. Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

- niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych oraz w samochodach,
- pilnego strzeżenia akt,
- nieużywania powtórnie dokumentów zadrukowanych jednostronnie,
- udostępniania danych osobowych pocztą elektroniczną tylko po uzyskaniu pisemnej zgody osoby której dotyczą
- niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej,
- niszczenia w niszczarce lub chowania do szaf wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy,
- niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
- zachowania tajemnicy danych, w tym także wobec najbliższych,
- chowania do szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy,
- zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych,

- zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,

- zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza w skrytce. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym pracowników sprzątających, celem uniknięcia zagubienia lub wyrzucenia dokumentów.

VII.ODPOWIEDZIALNOŚĆ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Niezastosowanie się do prowadzonej przez ADO Polityki, 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.

2. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej i /lub cywilnej.

4. VIII.Zabezpieczenia danych osobowych

1. Zabezpieczenia danych osobowych :

Tradycyjne	Nośniki	Informacji
Rodzaj danych	Typ nośnika	Zabezpieczenie
Dane osobowe	Papierowa dokumentacja	Przechowywane v szufladach zamyka osobnym pomiesz maja jedynie osob
Umowy z kontrahentami	Papierowa dokumentacja	Przechowywane v w pomieszczeniach zmykanych w pom do którego nie maj niupoważnione
Umowy z podmiotami przetwarzającymi	Papierowa dokumentacja	Przechowywane v w pomieszczeniach zmykanych w pom do którego nie maj nieupoważnione

VIII.FIZYCZNE ŚRODKI OCHRONY DANYCH OSOBOWYCH

1. Fizyczną ochronę danych i ich przetwarzania realizuje się poprzez::

- przetwarzanie danych osobowych w ściśle określonych miejscach do tego przeznaczonych, i tak dane osobowe uczniów wszystkie urządzenia zabezpieczone są hasłem przed osobami nieupoważnionymi

- Cała jednostka jest zamykana poprzez zastosowanie wysokiej jakość zamków drzwiowych, do których klucze posiadają tylko uprawnione osoby, oraz systemu alarmowego który jest uruchamiany na czas zamknięcia jednostki

- Dokumentacja papierowa w czasie otwarcia jednostki zawsze jest chowana do zamykanych na klucz szuflad w pomieszczeniu na zapleczu do którego może wejść wyłącznie upoważniona osoba, podczas zamknięcia jednostki szuflady z dokumentacją są zamykane na klucz

- Okna w jednostce są zabezpieczone na stałe i nie można ich otworzyć co ryzyko dostania się osób nieupoważnionych niweluje do zera,

- Wszystkie pomieszczenia wyposażone są w sprzęty oraz meble biurowe dające gwarancję bezpieczeństwa dokumentacji (szafy, biurka zamykane na klucz),

- Zapewniona jest odpowiednia organizacja stanowisk pracy osobom, które przetwarzają dane osobowe, tak by stanowisko nie pozostawało bez nadzoru

- dane osobowe po zakończeniu pracy przechowywane są w zamykanych na klucz meblach biurowych.

2. Niezależnie od niniejszych ustaleń mają zastosowanie wszelkie inne regulaminy.

IX. TECHNICZNE ŚRODKI OCHRONY DANYCH OSOBOWYCH

1. Techniczną ochronę danych i ich przetwarzania realizuje się poprzez:

- Zastosowanie wykonanych z materiałów nieprzezroczystych teczek oraz segregatorów, w których przechowywane są dane osobowe,

- Oznaczenie teczek oraz segregatorów, w których przechowywane są dane osobowe w sposób utrudniający identyfikacje ich zawartości osobom nieupoważnionym,

- Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem dostępu,

- zastosowanie wygaszaczy ekranu w przypadku nieaktywności użytkownika,

- Zastosowano blokadę hasłem podczas dłuższej nieaktywności użytkownika,

- zastosowanie na komputerach użytkowników bazy danych programów antywirusowych,

- wykonywanie kopii zapasowych przetwarzanych baz danych zapisywane na nośnikach danych osobowych.

- Niszczenie zapisków dotyczących osób fizycznych, czy dokumentacji , kopii dokumentów następuje poprzez fizyczne zniszczenie w niszczarce tak by nie można było odczytać jakiejkolwiek informacji

X. OCHRONA SPRZĘTU INFORMATYCZNEGO I OPROGRAMOWANIA

1. Sprzęt informatyczny i oprogramowanie podlega właściwej ochronie opisanej poniżej .

2. Sprzęt informatyczny oraz oprogramowanie wykorzystywane w systemach informatycznych muszą być zgodne z przepisami prawa i powinny być zgodne z najlepszymi praktykami.

3. System informatyczny może składać się wyłącznie z przetestowanego, formalnie dopuszczonego do eksploatacji sprzętu i oprogramowania.

4. Sprzęt i oprogramowanie powinny być eksploatowane, serwisowane i wycofywane z eksploatacji z zachowaniem właściwych procedur bezpieczeństwa.

5. Oprogramowanie instalowane w systemach informatycznych musi być legalne.

6. Wszelkie oprogramowanie musi być użytkowane z poszanowaniem praw własności intelektualnej, a w szczególności zgodnie z ustawą o prawie autorskim i prawach pokrewnyc

7. Sprzęt wchodzący w skład systemów informatycznych musi być objęty odpowiednią ochroną fizyczną.

8. Komputery i inne urządzenia przenośne, muszą być zabezpieczone.

9. Osoby korzystające z urządzeń przenośnych muszą być świadome zagrożeń i zobowiązane są do zachowania należytej staranności w celu zapewnienia ich bezpieczeństwa.

10. Zabrania się używania komputerów i urządzeń przenośnych zawierających informacje stanowiące tajemnicę bez zapewnienia ich właściwej ochrony poprzez zastosowanie obowiązujących środków organizacyjno-technicznych i prawnych .

11. 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.

12. Sporządzanie kopii zapasowych następuje codziennie.

13. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko za zgodą osoby której dotyczą.

14. Pocztę elektroniczną otwieramy z dużą rozwagę, niewiadomego pochodzenia poczty nie otwieramy tak jak i załączników, które mogą zawierać wirusy, tylko usuwamy ją w całości. Jeżeli nie wiesz od kogo jest poczta lub wzbudzi ona Twoją wątpliwość nigdy nie otwieraj załączników w niej zawartych i natychmiast zawiadom swojego przełożonego.

15. Przed atakami z sieci zewnętrznej wszystkie komputery (w tym także przenośne) chronione są środkami dobranymi przez ADO..

16. Wszystkie nośniki informacji podlegają właściwej ochronie stosownie do klasyfikacji informacji, na wszystkich etapach ich używania, od momentu zapisu informacji, aż do momentu wycofywania z użycia lub fizycznego zniszczenia .

17. Za zapewnienie właściwej ochrony nośników informacji odpowiada ich użytkownik.

18. Osoby korzystające z nośników informacji powinny być świadome zagrożeń, i zobowiązane są do zachowania należytej staranności poprzez zastosowanie obowiązujących środków organizacyjno-technicznych i prawnych.

19. Urządzenia przenośne oraz nośniki danych nie mogą być wynoszone z siedziby ADO oraz nie powinny być pozostawiane bez nadzoru w jednostce.

20. Nie można pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych ani też w samochodach jeżeli ADO wyraził zgodę na ich wyniesienie poza jednostkę.

21. 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.

22. W domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do ADO.

XI. ZARZĄDZANIE INCYDENTAMI

1. Celem zarządzania incydentami bezpieczeństwa jest redukcja ryzyka wystąpienia podobnych incydentów w przyszłości. Jednym z elementów zarządzania ryzykiem jest bieżące monitorowanie zagrożeń oraz okresowa kontrola celowości, adekwatności działań minimalizujących ryzyko.

2. ADO prowadzi działania wyjaśniające związane z incydentami bezpieczeństwa.

3. Działania, o których mowa w pkt 2, mają w szczególności na celu:

- minimalizację skutków zdarzenia,
- wyjaśnienie okoliczności zdarzenia,
- zabezpieczenie dowodów zdarzenia,
- doprowadzenie do sytuacji umożliwiającej dalsze przetwarzanie danych w systemie informatycznym,

4. Skutkiem wystąpienia zagrożenia może być:

- Uszkodzenie zbiorów danych,
- Utrata danych przetwarzanych przez jednostkę,

- Utrata poufności, integralności, dostępności, rozliczalności lub autentyczności danych,

- Zniszczeni, utracenie, zmodyfikowanie nieuprawnione, ujawnienie lub nieuprawniony dostęp do danych osobowych przechowywanych, archiwizowanych lub przesyłanych

5. System zarządzania ryzykiem jest zbudowany w sposób, który zapewnia prawidłowe działanie na każdym etapie, tj. zapobiegania, monitorowania oraz kontroli.

6. Polecenia ADO wydawane w czasie realizacji zadań wynikających z pkt 2 są priorytetowe i winny być wykonywane przed innymi.

7. Odmowa udzielania wyjaśnień lub współpracy z ADO traktowana jest, jako ciężkie naruszenie obowiązków pracowniczych.

XII. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Naruszeniem ochrony danych osobowych w rozumieniu Polityki jest każde zdarzenie, zależne jak i niezależne od woli ludzkiej, powodujące zagrożenie bezpieczeństwa danych osobowych, w szczególności :

- prowadzące do utraty integralności danych (np. pozostawianie dokumentów zawierających dane w miejscach powszechnie dostępnych)

- zagrażające poufności danych (np. przesyłanie danych drogą elektroniczną bez zabezpieczenia dostępu do plików)

- zagrażające rozliczalności danych (np. korzystanie przez kilka osób z jednego hasła dostępu)

2. Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

- stwierdzono naruszenie obowiązujących przepisów wewnętrznych,

- stwierdzono naruszenie obowiązujących przepisów prawa,

- stwierdzono naruszenie zabezpieczeń fizycznych lub informatycznych,

- stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,

- inne okoliczności wskazujące, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych przez jednostkę

3. Administrator w przypadku naruszenia ochrony danych osobowych bez zbędnej zwłoki w miarę możliwości nie później niż w terminie 72 h po stwierdzonym naruszeniu zgłasza je chyba że mało prawdopodobne jest by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

4. Zgłoszenie wysyłane później niż po 72 h musi zawierać wyjaśnienie przyczyn opóźnienia.

5. W zgłoszeniu winny zaleźć się informacje o:

- 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;

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

- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

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

5. Każdy incydent musi zostać wyjaśniony i opisany.

6. Procedura postępowania w przypadku naruszenia bezpieczeństwa danych załącznik nr. 15

XVI. POSTANOWIENIA KOŃCOWE

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

2. Każdej osobie upoważnionej do przetwarzania danych ADO udostępnia politykę bezpieczeństwa oraz procedury postępowania ochrony danych osobowych.

3. Polityka wchodzi w życie z dniem 25.05.2018

XVII. WZORY I PROCEDURY

A. ZGODY NA WYKORZYSTANIE WIZERUNKU I ZDJĘĆ DLA CELÓW REKLAMOWYCH ZAŁ. NR. 2

Czy zgadzasz się na przetwarzanie Twoich (Pana / Pani) danych osobowych zamieszczonych w niniejszym formularzu przez nas : ..... z siedzibą w ..... poprzez publikację ich na stronie internetowej www.... oraz na naszym profilu na Facebooku i/lub Instagramie , bez ograniczeń czasowych, nieodpłatnie w celu reklamowania naszych usług oraz metod leczniczych

Niniejsza zgoda będzie obejmować przetwarzanie danych osobowych poprzez wykorzystanie w postach Pani/Pana :

1/.Zdjęcia fotograficzne z zajęć oraz wykonane prace

2/.Inne wymienić : .....

Może Pan / Pani odwołać swoją zgodę pisemnie, i od daty wpłynięcia takiego oświadczenia Pan/Pani dane nie będą już przetwarzane w celach wskazanych w niniejszym formularzu. Odwołanie zgody nie będzie skutkowało usunięciem wizerunku z nośników elektronicznych oraz w materiałach reklamowych już wykorzystanych lub upublicznionych.

Ja ..... PESEL .....wyrażam zgodę zgodnie z zaznaczonym zakresem pkt. .....

.....

data podpis

B. INFORMOWANIE PISEMNE O PRAWACH I OBOWIĄZKACH -ZAŁ. NR.2

INFORMACJA

o przetwarzaniu danych osobowych

Informacja o przetwarzaniu Pana/Pani danych osobowych

1.Niniejszym pragniemy poinformować iż przetwarzamy Pana/Pani dane osobowe. Administratorem Danych Osobowych jest :

2.W celu realizacji umowy będziemy przetwarzać Pana / Pani dane osobowe z następujących kategorii :

A.Podstawowe dane identyfikacyjne : imię i nazwisko, adres zamieszkania , telefon, e-mail

2.Pana / Pani dane możemy udostępnić następującym kategoriom podmiotów :

- Księgowym - w zakresie wystawionych rachunków

5.Pana/Pani dane pozyskane w celu realizacji umowy przechowujemy przez okres 20 lat.

6.Panu / Pani przysługują prawa :

- Uzyskania potwierdzenia czy przetwarzamy Pana/Pani dane osobowe a jeżeli ma to miejsce do uzyskania dostępu do tych danych po weryfikacji tożsamości

- Prawo dostępu do swoich danych oraz otrzymania ich kopii, po weryfikacji tożsamości

- Do nieodpłatnej pierwszej kopii przetwarzanych danych, wydanie kolejnych kopii jest odpłatne,

- Prawo do sprostowania (poprawienia) swoich danych

- Prawo do bycia zapomnianym

- Prawo do ograniczenia przetwarzania danych

- Prawo do cofnięcia zgody na przetwarzanie danych osobowych ; W każdej chwili może Pan/Pani cofnąć zgodę na przetwarzanie danych osobowych.Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania , którego dokonaliśmy na podstawie Pana/Pani zgody przed wycofaniem.

- Prawo do wniesienia skargi do organu nadzorczego ; Jeżeli Pan/ Pani uważa , że przetwarzamy Twoje dane osobowe niezgodnie z prawem, może złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych .

7.Weryfikacji tożsamości dokonuje się poprzez kontrolę okazanego przez Pana/Panią dokumentu potwierdzającego tożsamość zawierającego co najmniej zdjęcie, imię i nazwisko oraz PESEL lub w przypadku jego braku inny numer jednoznacznie identyfikujący Pacjenta. Dokumentem potwierdzającym tożsamość jest w szczególności: dowód osobisty, legitymacja studencka, prawo jazdy, paszport.

8. Zapoznałam/łem się z informacją o przetwarzaniu Moich/ mojego syna /córki danych osobowych w dniu .....

Imię i nazwisko : .....

C. ZGODNIE Z ART. 15 RODO - WZÓR - INFORMACJA O ZAKRESIE PRZETWARZANIA DANYCH - ZAŁ. NR. 9

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

Niniejszym informuję Pana/ Panią w związku z Pani/Pana żądanie dotyczącym informacji czy są przetwarzane Pana/Pani dane osobowe iż :

Pana/ Pani dane są przetwarzane : w celu wykonania umowy , dane przetwarzane to : imię i nazwisko, adres zamieszkania, telefon, e-mail , okres przechowywania powyższych danych to 20 lat.

Ma Pani/Pan prawo do żądania sprostowania swoich danych osobowych.

D. WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH (PRACOWNICY)STANOWI ZAŁ. NR. 13

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)

Z dniem .....nadaję upoważnienie Pani/Panu :

stanowisko :

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

Jednocześnie zobowiązuję Pana/ Panią do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem, przepisami RODO, przepisami prawa oraz z polityką ochrony danych osobowych.

Okres trwania upoważnienia: do odwołania

Osoba upoważniona zobowiązana jest do zachowania w tajemnicy wszelkich informacji o danych osobowych uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych.Obowiązek ten istnieje również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....

Podpis upoważniającego

Oświadczam, że akceptuje zasady powyższego upoważnienia i zobowiązuje się do przestrzegania jego warunków.

.....

Data podpis upoważnionego

E. WZÓR OŚWIADCZENIA O ZACHOWANIU POUFNOŚCI PRZETWARZANYCH DANYCH -ZAŁ. NR 14

Oświadczenie o zachowaniu poufności

Ja niżej podpisany(a).....,

w dniu .....zostałem(am) zapoznany(a) z przepisami 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 polityką ochrony danych osobowych .

Niniejszym zobowiązuję się przestrzegać zasad oraz procedur wynikających z powszechnie obowiązujących przepisów prawa, Polityki Ochrony Danych Osobowych i w zakresie ochrony danych osobowych.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania, do których mam lub będę miał(a) dostęp w związku z wykonywaniem obowiązków wynikających ze stosunku zatrudnienia, w trakcie jego trwania jak i po ustaniu.

Oświadczam, ze zostałem(am) pouczony o odpowiedzialności za niedopełnienie obowiązków wynikających z niniejszego oświadczenia.

Naruszenie przepisów ochrony danych jest traktowane jako ciężkie naruszenie obowiązków pracowniczych.

Naruszenie przepisów ochrony danych w przypadku umowy cywilnoprawnej wiąże się dla tej osoby z odpowiedzialnością karną , cywilną oraz możliwością dochodzenia odszkodowań za naruszenie ochrony danych osobowych.

.....

Imię i nazwisko / data

F. PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH ZAŁ. NR. 15

1. Gdy stwierdzisz iż doszło do naruszenia bezpieczeństwa danych poprzez :

   a. Uszkodzenie zbiorów danych,

   b. Utrata danych przetwarzanych przez jednostkę,

   c. Utrata poufności, integralności, dostępności, rozliczalności lub autentyczności danych,

   d. Zniszczeni,

   e. utracenie,

   f. zmodyfikowanie nieuprawnione,

   g. ujawnienie lub nieuprawniony dostęp do danych osobowych przechowywanych, archiwizowanych lub przesyłanych

Natychmiast zawiadom przełożonego .

2. Natychmiast zabezpiecz miejsce pracy i/lub zawiadom właściwe służby (Policję, Straż Pożarną , informatyka)

3. Postępuj zgodnie z poleceniami przełożonego.

4. Zapisz datę i godzinę stwierdzonego naruszenia i opisz okoliczności zdarzenia.

5. Jeżeli jest to możliwe przystąp do ustalenia danych osób które mogły zostać dotknięte naruszeniem bezpieczeństwa danych.

6. Informacje z pkt.4 i 5 przekaż przełożonemu.

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH*KSIEGOWOŚĆ

Zawarta w dniu ..... w

Pomiędzy :- Administratorem

A

Przetwarzającym

łącznie jako „ strony „ :

1. Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych danych osobowych (dalej zwanych danymi).

2. Przetwarzanie będzie wykonywane w okresie obowiązywania niniejszej umowy.

3. Przetwarzający prowadzi obsługę księgową oraz kadrową Administratora w związku z tym celem przetwarzania jest zrealizowanie przez Przetwarzającego obowiązków ustawowych dotyczących prawidłowego rozliczania księgowego Administratora i prowadzenia w sposób zgodny z prawem obsługi kadrowej pracowników Administratora.

4. Przetwarzanie obejmować będzie następujące rodzaje danych osobowych :

A. Dane Zwykłe :

- W zakresie pracowników : imię i nazwisko, PESEL, imiona rodziców , nazwisko panieńskie matki, adres e-mail, numer telefonu, adres zamieszkania, data urodzenia, NIP, seria i numer dowodu tożsamości, numer rachunku bankowego,

- W zakresie współpracowników : imię i nazwisko, NIP, adres zamieszkania ,

B. Dane szczególnych kategorii :

- dokumentacja medyczna pracownicza

- Orzeczenia o dopuszczalności do pracy

C. Dane dzieci :

- imię i nazwisko, PESEL, data urodzenia

5. Przetwarzanie danych będzie dotyczyć następujących kategorii osób :

- pracownicy Administratora

- Klienci usług Administratora

- Kontrahenci dostawcy Administratora

6. Obowiązki Przetwarzającego :

a. Przetwarzający przetwarza dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora

b. Przetwarzający oświadcza iż nie przekazuje danych do państwa trzeciego. Przetwarzający oświadcza iż nie korzysta z podwykonawców którzy przekazują dane poza Europejski Obszar Gospodarczy.(EOG)

c. Jeżeli przetwarzający ma zamiar lub obowiązek przekazywać dane poza EOG informuje o tym Administratora w celu umożliwienia mu podjęcia decyzji i działań zapewniających przetwarzanie danych zgodnie z prawem lub zakończenia powierzenia przetwarzania.

d. Przetwarzający uzyskuje od osób , które zostały upoważnione do przetwarzania danych osobowych objętych niniejszą umową udokumentowane zobowiązanie do zachowania tajemnicy i poufności.

e. Przetwarzający zapewnia ochronę danych i podejmuje środki ochrony danych o których mowa w art. 32 RODO.

f. Przetwarzający zobowiązuje się wobec Administratora do odpowiadania na żądania osoby, w zakresie wykonywania praw określonych w rozdziale III RODO (prawa jednostki.

g. Przetwarzający współpracuje z Administratorem przy wykonywaniu jego obowiązków , w szczególności : ochrona danych, zgłaszanie naruszeń , realizacja praw jednostki)

h. Przetwarzający zobowiązuje się prowadzić RCPD i udostępnia rejestr na każde żądanie Administratora.

i. Przetwarzający zapewnia szkolenia z zakresu ochrony danych osobowych dla osób upoważnionych w jego imieniu do przetwarzania danych.

7. Przetwarzający przedstawił pisemnie Administratorowi informacje i dokumenty dotyczące wdrożonych środków ochrony danych w tym środków technicznych oraz organizacyjnych i jednocześnie przetwarzający oświadcza iż dane przez niego przetwarzane są zabezpieczone w sposób wystarczający by ryzyko naruszenia danych było znikome. Dokumentacja w tym zakresie jest dowodem spełnienia wymogu rozliczalności.

8. Przetwarzający powiadamia Administratora o każdym podejrzeniu naruszenia ochrony danych osobowych nie później niż w ciągu 24 godzin od pierwszego zgłoszenia i umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających oraz informuje o ustaleniach w zakresie naruszenia ochrony danych.

9. Przetwarzający przesyła powiadomienie o stwierdzonym naruszeniu wraz z dokumentacją dot. Tego naruszenia aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.

10. Administrator oświadcza że jest administratorem danych i jest uprawniony do ich przetwarzania w zakresie w jakim powierzył je Przetwarzającemu.

11. Przetwarzający oświadcza iz w ramach powierzonych mu czynności przetwarzania danych posiada niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmie należytego wykonania umowy.

12. Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków wynikających z RODO. Przetwarzający odpowiada za zastosowanie lub niezastosowanie właściwych środków bezpieczeństwa.

13. Umowa zostaje zawarta na czas nieokreślony z możliwością trzymiesięcznego wypowiedzenia niniejszej umowy w formie pisemnie.

14. Z chwilą rozwiązania niniejszej umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych mu danych i jest zobowiązany do

- usunięcia danych i poinformowaniu o tym Administratora wskazując datę i sposób usunięcia danych

- Usunięcia wszystkich kopii lub zwrotu danych chyba że Administrator postanowi inaczej lub przepisy nakazują dalej przechowywać dane

- Przetwarzający usunie dane po upływie 180 dni od zakończenia umowy chyba że Administrator poleci mu to uczynić wcześniej,

15. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron

16. Umowa podlega RODO i prawu polskiemu.

17. Jeżeli którykolwiek z zapisów byłby sprzeczny z obowiązującymi przepisami to zostaje on wyłączony przy obowiązywaniu pozostałych postanowień niniejszej umowy.

Administrator : Przetwarzający

R C P D Z AŁ. N R. 1 -

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

ADMINISTRATOR	
ADRES	
KRS/ CRIDG	CRIDG
NIP	
REGON	
TELEFON	

EMAIL	
STRONA WWW	
INSPEKTOR OCHRONY DANYCH	
ADRES	
TELEFON	
EMAIL	

REJESTR PRZETWARZAJĄCEGO

NAZWA POWIERZONEGO PROCESU	NAZWA PODMIOTU PRZETWARZAJĄCEGO DANE	ADRES I DANE KONTAKTOWE PODMIOTU PRZETWARZAJACEGO	Cel	CZYNNOŚCI PRZETWARZANIA W IMIENIU ADMINISTRATORA	TRANSFER DO PAŃSTWA TRZECIEGO	NAZWA PAŃSTWA TRZECIEG
Prowadzenie dokumentacji pracowniczej			Prowadzenie akt osobowych pracowników, obowiazki ubezpieczeniowe, proces zatrudnienia	Dane osobowe pracowników, imię inazwisko, PESEL, imiona rodziców , NIP, adres zamieszkania, dane dzieci , konto bankowe	Nie	Nie
Prowadzenie rozliczeń księgowych - rachunki i faktury			Rozliczenia finansowe, wykonanie obowiązków podatkowych	Dane pacjentów,współpracowników ,kontrahentów niezbędne do wystawienia rachunku lub faktury	Nie	Nie

RCPD

	REJESTR CZYNNOŚCI	**DANYCH**		
CZYNNOŚCI PRZETWARZANIA	CEL	PODSTAWA PRAWANA PRZETWARZANIA	KATEGORIA OSÓB KTÓREJ DOTYCZY	KATEGORIA DANYCH
POBIERANIE danych	Wykonanie umowy	Umowa	Uczeń	Imię i nazwisko Adres zamieszkania Telefon Email
WYSTAWIANIE I WYDAWANIE RACHUNKÓw	Wykonanie umowy	Umowa	Uczen	Imię i nazwisko Adres zamieszkania
PRZEKAZYWANIE INFORMACJI FINANSOWYCH	Wykonywanie obowiązków skarbowych	Ordynacja podatkowa	Uczen	Imię i nazwisko Adres zamieszkania Nip
NISZCZENIE DOKUMENTÓW	Trwałe zniszczenie danych		Uczeń	Wszystkie kategorie danych

REJESTR CZYNNOŚCI						
CZYNNOŚCI PRZETWARZANIA	SPOSÓB PRZETWARZANIA	SPOSÓB POZYSKIWANIA	OKRES PRZECHOWYWANIA	ŚRODKI BEZPIECZEŃSTWA	DOKUMENTACJA ODPOWIEDNICH ZABEZPIECZEŃ	DATA AKTUALIZACJI
POBIERANIE DANYCH	wpisywanie, przechowywanie, archiwizowanie, przeglądanie	Bezpośredni	1 rok	Przechowywane i archiwizowane w programach , zabezpieczenie programów hasłem/kodem, w formie papierowej przechowywanie w teczkach i zamkniętych pomieszczeniach zabezpieczonych kodem	Oprogramowanie systemu, fizyczne, szafki, pomieszczenia chronione kodem dostępu	Maj 2018

WYSTAWIANIE I WYDAWANIE RACHUNKÓW	wpisywanie, przechowywanie, archiwizowanie, przeglądanie	Bezpośredni	5lat	Przechowywane i archiwizowane w programach , zabezpieczenie programów hasłem/kodem, w formie papierowej przechowywanie w teczkach i zamkniętych pomieszczeniach zabezpieczonych kodem, przechowywane przez podmiot przetwarzający	Oprogramowanie systemu, fizyczne, szafki, pomieszczenia chronione kodem dostępu	Maj 2018
PRZEKAZYWANIE INFORMACJI FINANSOWYCH	Przechowywanie, archiwizowanie,przegladanie	Bezpośredni, e-mail	5lat	Przechowywane i archiwizowane w programach , zabezpieczenie programów hasłem/kodem, w formie papierowej przechowywanie w teczkach i zamkniętych pomieszczeniach zabezpieczonych kodem, przechowywane przez podmiot przetwarzający	Oprogramowanie systemu, fizyczne, szafki, pomieszczenia chronione kodem dostępu	Maj 2018
ODBIERANIE POCZTY E-MAIL	Przechowywanie, archiwizowanie,przegladanie	Bezpośredni	W zależności od kategorii przesyłanych/odbieranych informacji w e-mailach	Przechowywane i archiwizowane w programach , zabezpieczenie programów hasłem/kodem, w formie papierowej przechowywanie w teczkach i zamkniętych pomieszczeniach zabezpieczonych kodem	Oprogramowanie systemu, fizyczne, szafki, pomieszczenia chronione kodem dostępu	Maj 2018
WYSYŁANIE POCZTY E-MAIL	Przechowywanie, archiwizowanie,przegladanie	Bezpośredni	W zależności od kategorii przesyłanych/odbieranych informacji w e-mailach	Przechowywane i archiwizowane w programach , zabezpieczenie programów hasłem/kodem, w formie papierowej przechowywanie w teczkach i zamkniętych pomieszczeniach zabezpieczonych kodem	Oprogramowanie systemu, fizyczne, szafki, pomieszczenia chronione kodem dostępu	Maj 2018
NISZCZENIE DOKUMENTÓW		Bezpośredni				Maj 2018

D. ANALIZA RYZYKA

ZAGROŻENIA DLA BEZPIECZEŃSTWA INFORMACJI

Zagrożenie	Przyczyna	Zabezpieczenie	Skutek
Pożar	niezależna/na skutek działanie niezgodnego z BHP	Szkolenie BHP dotyczące bezpieczeństwa z obsługą i korzystanie z urządzeń elektrycznych, zabezpieczenie urządzeń przed przepięciami, kontrola kabli , przedłużaczy, gaszenie świeczek,	Utrata be danych o medyczny zdarzenia
Zalanie	niezależna/na skutek działanie niezgodnego z BHP	Szkolenie BHP dotyczące bezpieczeństwa z obsługą i korzystanie z urządzeń wodnych, nie pozostawianie odkręconych kranów , zabezpieczenie instalacji wodno-kanalizacyjnej	Utrata be danych o medyczny zdarzenia
Zniszczenie nośników danych	niezależna/na skutek działanie niezgodnego z BHP	Postępowanie zgodnie z procedurami	Utrata be danych o medyczny zdarzenia
Awaria urządzeń informatycznych	niezależna/na skutek działanie niezgodnego z procedurami		
Awaria programów	nieznana/ wirus	Oprogramowanie antywirusowe	Możliwoś zapasowy
Kradzież nośników	Włamanie, kradzież	System alarmowy, zabezpieczenia dokumentacji w pomieszczeniach zamykanych	Możliwoś zapasowy
Kradzież dokumentów	Kradzież	System alarmowy, zabezpieczenia dokumentacji w pomieszczeniach zamykanych	Możliwoś zapasowy
Niewłaściwe działanie urządzenia	Wirusy, uszkodzenie	Systematyczny seris urządzeń, oprogramowanieantywirusowe	Możliwoś zapasowy
Przeciążaenie systemu informatycznego	Niezależne	Serwis urządzeń sprawdzanie zapełnienia dysku	Możliwoś zapasowy
Nieautoryzowane wejście do programu	Włamanie do systemu	Hasła kody	Możliwoś zapasowy

Nieuprawnione kopiowanie oprogramowania	Wykorzystanie upoważnienia sprzecznie z jego podstawą	Kody, hasła	Wyciek d
Zniekształcenie danych	Błąd ludzki	Kody, hasła	Pomyłki
Uzycie nieautoryzowanego oprogramowania	Działanie niezgodne z prawem	Kody, hasła	Mozliwoś
Nielegalne przetważanie danych	działanie niezgodne z prawem	Kody, hasła	Wyciek d
Błąd użytkownika	Błąd ludzki	Procedury, upoażnienia, szkolenia	Możliwoś zapasowy
Naruszenie uprawnień	Błąd ludzki	Procedury, upoażnienia, szkolenia	Możliwoś zapasowy
Fałszowanie uprawnień	Działanie niezgodne z prawem	Kody, hasła	Wyciek d
Odmowa działania	Błąd umyślny lub nieumyslny	Procedury, upoażnienia, szkolenia	Brak dost
Włamanie do systemu	Hakerstwo	Kody, hasła	Możliwoś zapasowy
Działanie osób wewnątrz jednostki niezgodne z zasadami i polityką.	Umyślne działanie	Kody, hasła, procedury, upowaznienia	wyciek, d

REJESTR NARUSZEŃ

	Zdarzenie	Zdarzenie
Opis naruszenia		
Data i godzina złoszenia		
data i godzina stwierdzenia naruszenia		
Okres którego naruszenie dotyczy		

Kategoria i liczba osób którego naruszenie dotyczy		
Zakres danych których dotyczy naruszeni		
źródło informacji o naruszeniu (kto zgłosił)		
Miejsce zdarzenia		
Okoliczności zdarzenia (opis , może zostać dołączony do rejestru na osobnej kartce z datą zdarzenia)		

opis skutków naruszenia		
Ryzyko naruszenia praw i wolności (brak/pomijalne/niskie/wysokie/ maxymalne)		
Opis naruszenia praw lub wolności		

Opis działań minimalizujących negatywne skutki		
Opis działań podjętych w celu wyeliminowania w przyszłości podobnych naruszeń		

Rezultat działań naprawczych		
Osoba odpowiedzialna za wdrożenie działań naprawczych		
Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobbowych (72 h od stwierdzenia naruszenia)		
kiedy wysłano powiadomienie do UODO (jeżeli było to konieczne)		
czy poinformowano organy ścigania i kiedy		
czy zachodzi obowiązek poinformowania osób których dane zostały naruszone		
Kiedy poinformowano osoby o naruszeniu ich danych i w jakiej formie		
Czy działania naprawcze zostały wdrożone		
Kiedy zakończono wdrażanie działań naprawczych		