Polityka Bezpieczeństwa Danych Osobowych

ISSA – Usługi Weterynaryjne

Świerżewski Piotr

Polityka Bezpieczeństwa

Administrator Danych Osobowych **Piotr Świerżewski**

z dniem **02.05.2018r.** wdraża w podmiocie o nazwie ***ISSA – Usługi Weterynaryjne Świerżewski Piotr***

dokument o nazwie ***„Polityka Bezpieczeństwa Danych Osobowych”*** , której zapisy regulują przetwarzanie danych osobowych w zgodzie z *Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE*, zwanego dalej RODO.

Zapisy tego dokumentu wchodzą w życie z dniem 25.05.2018r.

§1
Zadania Polityki

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w ***ISSA – Usługi Weterynaryjne Świerżewski Piotr*** określa metody przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia stosowania zasad wg art. 5 ust. 1 RODO, a mianowicie:

1) zgodności z prawem, rzetelności i przejrzystości;
2) ograniczenia celu przetwarzania;
3) minimalizacji danych;
4) prawidłowości danych;
5) ograniczenia przechowywania danych;
6) integralności i poufności danych;
7) rozliczalności.

2. Dokument ten służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Dotyczy on danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§2
Definicje

Ilekroć w „Polityce Bezpieczeństwa” jest mowa o:

1. *danych osobowych* – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
2. *przetwarzaniu danych* – rozumie się przez to operację lub zestaw operacji wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany bądź niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie,

rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

3. *systemie informatycznym* – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
4. *zabezpieczeniu danych w systemie informatycznych* – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed ich nieuprawnionym przetwarzaniem;
5. *usuwaniu danych* – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
6. *administratorze danych osobowych* – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
7. *zbiorze danych* – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
8. *podmiocie* – rozumie się przez to firmę, której właścicielem jest administrator;
9. *podmiocie przetwarzającym* – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane w imieniu administratora.

§3
Inspektor Ochrony Danych Osobowych

1. Administrator Danych w podmiocie ISSA – Usługi Weterynaryjne Świerżewski Piotr po przeanalizowaniu sytuacji związanej z przetwarzaniem danych osobowych uwidocznionej w Rejestrze Czynności Przetwarzania danych (*zał. 1*) i skonfrontowaniu jej z art. 37 ust. 1 RODO, uznał, że **nie istnieje obowiązek** wyznaczenia **inspektora ochrony danych**, gdyż:
   1) w rozumieniu ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych nie przetwarzamy danych jako organ lub podmiot publiczny;
   2) operacje przetwarzania nie wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
   3) główna działalność firmy nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych.

2. W związku z powyższym inspektor ochrony danych osobowych **nie został wyznaczony.**

§4
Środki techniczne i organizacyjne

1. W podmiocie ISSA – Usługi Weterynaryjne Świerżewski Piotr dane osobowe są zbierane, przetwarzane i przechowywane zgodnie z prawem, rzetelnie i w przejrzysty sposób, w konkretnych i prawnie uzasadnionych celach i za zgodą osoby, której dane dotyczą, wykazując adekwatność do celu. Są one na bieżąco poprawiane i uaktualniane, a przechowywanie ich odbywa się przez okres nie dłuższy niż jest to niezbędne i wymagane odrębnymi przepisami. Administrator Danych, aby zapewnić integralność i poufność wprowadza środki techniczne i organizacyjne chroniące przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem po przeanalizowaniu możliwych zagrożeń.
2. W ślad za tabelą nr 5 wykonanej Analizy Ryzyka – *zał. 2*, która określa ryzyko wystąpienia zagrożeń – Administrator Danych stwierdza, iż zastosowanie zabezpieczeń i środków zaradczych jest konieczne w przypadku wystąpienia ryzyka na poziomach 2 – średnie oraz 3 – duże i postanawia w przypadku:
    1) internetowego konta mailowego, przy pomocy którego wysyłane są dane ze stanowiska na stanowisko lub pomiędzy Administratorem a podmiotami przetwarzającymi na podstawie umów powierzenia, wprowadzić następujące środki techniczne i organizacyjne:
        a) dostęp do konta mają tylko i wyłącznie osoby upoważnione na podstawie pisemnego upoważnienia wydanego przez Administratora (Rejestr upoważnień – *zał. 3*);
        b) osoby upoważnione zostały przeszkolone w aspekcie ochrony danych osobowych;
        c) osoby upoważnione zobowiązały się na piśmie o zachowaniu poufności danych osobowych pod rygorem kar wynikających z odrębnych przepisów;
        d) osoby upoważnione do przesyłu danych używają tylko i wyłącznie firmowego konta mailowego założonego w serwisie Onet, który zapewnia szyfrowanie wiadomości protokołem SSL (potwierdzone przez Onet mailowo – wydruk maila *zał. 4*);
        e) osoby upoważnione przesyłają tylko niezbędne dane, konieczne do wykonywania obowiązków pracowniczych;
        f) dostęp do konta zabezpieczony jest hasłem o wysokim bezpieczeństwie, które znają tylko i wyłącznie osoby upoważnione;
        g) dostęp do sieci wifi zabezpieczony hasłem o wysokim bezpieczeństwie;
        h) dostęp do systemu komputerowego zabezpieczony hasłem o wysokim bezpieczeństwie;
        i) po skopiowaniu koniecznych danych wiadomości je zawierające są usuwane, a użytkownik niezwłocznie wylogowuje się z konta;
        j) dane przesyłane są zabezpieczane dodatkowo hasłem przekazywanym telefonicznie po wysłaniu maila;

k) system chroniony jest programem antywirusowym i zaporą firewall;
l) komputery są umieszczone w pomieszczeniach zamykanych na klucz, chronionych systemem alarmowym, grupą interwencyjną lub kratami w oknach;
m) klucze udostępniane są tylko osobom upoważnionym zgodnie z wprowadzoną polityką kluczy (*zał. 5*);
n) komputery są rozmieszczone tak, aby uniemożliwić wgląd dla osób nieuprawnionych lub stosowane filtry prywatyzujące;
o) stosuje się wygaszacz ekranu z ponownym logowaniem się do systemu w razie dłuższej nieaktywności;
p) podpisano umowy powierzenia przetwarzania danych osobowych z podmiotami przetwarzającymi wraz ze zobowiązaniem o zapewnieniu odpowiednich środków technicznych i organizacyjnych dla ochrony powierzonych danych osobowych (Rejestr umów powierzenia *zał. 6*);
q) wprowadzono politykę czystego ekranu (*zał. 7*) i biurka (*zał. 8*).

2) ewidencji papierowej, za której pomocą są prowadzone prawie wszystkie rejestry firmy, w tym akta osobowe, które ze względu na konieczność długiego czasu przechowywania wymagają szczególnej ochrony, wprowadzić następujące środki techniczne i organizacyjne:
a) dostęp do rejestrów mają tylko i wyłącznie osoby upoważnione na podstawie pisemnego upoważnienia wydanego przez Administratora;
b) osoby upoważnione zostały przeszkolone w aspekcie ochrony danych osobowych;
c) osoby upoważnione zobowiązały się na piśmie o zachowaniu poufności danych osobowych pod rygorem kar wynikających z odrębnych przepisów;
d) osoby upoważnione korzystają z danych tylko w zakresie niezbędnym do wykonywania obowiązków pracowniczych;
e) rejestry po skończonej pracy umieszczane są w szafkach zamykanych na klucz;
f) rejestry są umieszczone w pomieszczeniach zamykanych na klucz, chronionych drzwiami antywłamaniowymi oraz systemem alarmowym i grupą interwencyjną;
g) klucze udostępnione są tylko osobom upoważnionym, zgodnie z wprowadzoną polityką kluczy;
h) wdrożono procedury oraz zabezpieczenia przeciwpożarowe;
r) akta osobowe przechowywane są w zamykanym na klucz pomieszczeniu, znajdującym się na drugiej kondygnacji w metalowej szafie ognioodpornej z zamkiem szyfrowym;
s) podpisano umowy powierzenia przetwarzania danych osobowych z podmiotami przetwarzającymi wraz ze zobowiązaniem o zapewnieniu

odpowiednich środków technicznych i organizacyjnych dla ochrony powierzonych danych osobowych (Rejestr umów powierzenia *zał. 6*);

i) wprowadzono politykę czystego biurka (*zał. 8*), ekranu (*zał. 7*) i samochodu (*zał. 9*);
j) po okresie koniecznego przechowywania danych, są one skutecznie niszczone przy pomocy niszczarki.

3) programu Infor system, przy pomocy którego prowadzona jest księgowość i sprawy kadrowe firmy, wprowadzić następujące środki techniczne i organizacyjne:
   a) podpisano umowę powierzenia przetwarzania danych osobowych z Biurem Rachunkowym Daniel Milewski wraz ze zobowiązaniem o zapewnieniu przez podmiot przetwarzający odpowiednich środków technicznych i organizacyjnych dla ochrony powierzonych danych osobowych (Rejestr umów powierzenia *zał. 6*).
4) program internetowego konta bankowego, przy pomocy którego prowadzone są rozliczenia z pracownikami, wprowadzić następujące środki techniczne i organizacyjne:
   a) dostęp do konta bankowego posiada tylko i wyłącznie Administrator danych osobowych i Pełnomocnik posiadający upoważnienie, zobowiązanie do poufności i szkolenie w zakresie ochrony danych osobowych;
   b) dostęp do konta zabezpieczony jest hasłem o wysokim bezpieczeństwie;
   c) komputery są rozmieszczone tak, aby uniemożliwić wgląd dla osób nieuprawnionych;
   d) stosuje się wygaszacz ekranu z ponownym logowaniem się do systemu w razie dłuższej nieaktywności;
   e) konto bankowe zapewnia samoczynne wylogowanie użytkownika w przypadku dłuższej nieaktywności;
   f) dostęp do sieci wifi zabezpieczony hasłem o wysokim bezpieczeństwie;
   g) dostęp do systemu komputerowego zabezpieczony hasłem o wysokim bezpieczeństwie;
   h) komputery są umieszczone w pomieszczeniach zamykanych na klucz, chronionych systemem alarmowym, grupą interwencyjną lub kratami w oknach;
   i) klucze udostępniane są tylko osobom upoważnionym zgodnie z wprowadzoną polityką kluczy;
   j) komputery są rozmieszczone tak, aby uniemożliwić wgląd dla osób nieuprawnionych lub stosowne filtry prywatyzujące;
   k) wprowadzono politykę czystego ekranu i biurka.
5) program Klinika XP, przy pomocy którego wypełniany jest obowiązek prowadzenia dokumentacji lekarsko-weterynaryjnej, wprowadzić następujące środki techniczne i organizacyjne:

a) dostęp do danych w programie mają tylko i wyłącznie osoby upoważnione na podstawie pisemnego upoważnienia wydanego przez Administratora;
b) osoby upoważnione zostały przeszkolone w aspekcie ochrony danych osobowych;
c) osoby upoważnione zobowiązały się na piśmie o zachowaniu poufności danych osobowych pod rygorem kar wynikających z odrębnych przepisów;
d) osoby upoważnione w ramach prowadzenia dokumentacji lekarsko-weterynaryjnej przetwarzają dane w formie papierowej oraz w formie elektronicznej wyłącznie w programie Klinika XP;
e) w programie przetwarzane są tylko i wyłącznie dane niezbędne do prowadzenia dokumentacji lekarsko-weterynaryjnej, przetwarzanie innych danych niż w/w wymaga pisemnej zgody osoby, której dane dotyczą;
f) dostęp do programu zabezpieczony jest hasłem o wysokim bezpieczeństwie, które znają tylko i wyłącznie osoby upoważnione i które podlega zmianie co 30 dni;
g) każdy upoważniony posiada własny login i hasło dostępowe do przetwarzanych danych;
h) dostęp do sieci wifi zabezpieczony hasłem o wysokim bezpieczeństwie;
i) dostęp do systemu komputerowego zabezpieczony hasłem o wysokim bezpieczeństwie;
j) tworzone są kopie zapasowe zabezpieczone hasłem o wysokim bezpieczeństwie zmienianym co 30 dni na dyskach zewnętrznych;
k) dzięki dostosowywaniu programu do przepisów RODO (*zał. 21*) posiada on wszelkie niezbędne zabezpieczenia i możliwości wykonalności praw osób, których dane dotyczą;
l) system chroniony jest programem antywirusowym i zaporą firewall;
m) komputery są umieszczone w pomieszczeniach zamykanych na klucz, chronionych systemem alarmowym, grupą interwencyjną lub kratami w oknach;
n) klucze udostępniane są tylko osobom upoważnionym zgodnie z wprowadzoną polityką kluczy;
o) komputery są rozmieszczone tak, aby uniemożliwić wgląd dla osób nieuprawnionych lub stosowane filtry prywatyzujące;
p) stosuje się wygaszacz ekranu z ponownym logowaniem się do systemu w razie dłuższej nieaktywności;
q) po skończonej pracy użytkownik wylogowuje się niezwłocznie i wyłącza program wykonując archiwizację danych na dysku zewnętrznym;
r) po ustaniu koniecznego okresu przechowywania danych, są one anonimizowane przy pomocy środków, które zapewnia program;
s) komputery zabezpieczone są awaryjnym zasilaczem (UPS);
t) wdrożono procedury oraz zabezpieczenia przeciwpożarowe;
u) wprowadzono politykę czystego ekranu (*zał. 7*) i biurka (*zał. 8*).

6) program Word i Excel, przy pomocy których prowadzone są niektóre rejestry, wprowadzić następujące środki techniczne i organizacyjne:
   a) dostęp do danych w programach mają tylko i wyłącznie osoby upoważnione na podstawie pisemnego upoważnienia wydanego przez Administratora;
   b) osoby upoważnione zostały przeszkolone w aspekcie ochrony danych osobowych;
   c) osoby upoważnione zobowiązały się na piśmie o zachowaniu poufności danych osobowych pod rygorem kar wynikających z odrębnych przepisów;
   d) w programach przetwarzane są tylko i wyłącznie dane niezbędne do prowadzenia dokumentacji wymaganej prawem, przetwarzanie innych danych niż w/w wymaga pisemnej zgody osoby, której dane dotyczą;
   e) dostęp do plików z rejestrami zabezpieczony jest hasłem o wysokim bezpieczeństwie, które znają tylko i wyłącznie osoby upoważnione;
   f) dostęp do sieci wifi zabezpieczony hasłem o wysokim bezpieczeństwie;
   g) dostęp do systemu komputerowego zabezpieczony hasłem o wysokim bezpieczeństwie;
   h) tworzone są kopie zapasowe zabezpieczone hasłem o wysokim bezpieczeństwie na dyskach zewnętrznych;
   i) dostęp do danych w tzw. chmurze zabezpieczony hasłem o wysokim bezpieczeństwie;
   j) system chroniony jest programem antywirusowym i zaporą firewall;
   k) komputery są umieszczone w pomieszczeniach zamykanych na klucz, chronionych systemem alarmowym, grupą interwencyjną lub kratami w oknach;
   l) klucze udostępniane są tylko osobom upoważnionym zgodnie z wprowadzoną polityką kluczy;
   m) komputery są rozmieszczone tak, aby uniemożliwić wgląd dla osób nieuprawnionych lub stosowane filtry prywatyzujące;
   n) stosuje się wygaszacz ekranu z ponownym logowaniem się do systemu w razie dłuższej nieaktywności;
   o) po skończonej pracy użytkownik niezwłocznie wyłącza program wykonując archiwizację danych na dysku zewnętrznym;
   p) po ustaniu koniecznego okresu przechowywania danych, są one skutecznie usuwane;
   q) komputery zabezpieczone są awaryjnym zasilaczem (UPS);
   r) wdrożono procedury oraz zabezpieczenia przeciwpożarowe;
   s) wprowadzono politykę czystego ekranu (*zał. 7*) i biurka (*zał. 8*).

3. Sporządzono wykaz poszczególnych pomieszczeń przetwarzania i przechowywania danych osobowych z wypisaniem zabezpieczeń w nich zastosowanych:

Lp.	Dokładny Adres	Dział użytkujący pomieszczenie	Rodzaj zastosowanego zabezpieczenia pomieszczenia
1.	Długobórz, ul. Zambrowska 5 18-300 Zambrów	Recepcja	- drzwi wejściowe zamykane na klucz z obu stron; -alarm; - grupa interwencyjna - Konsalnet
2.	Długobórz, ul. Zambrowska 5 18-300 Zambrów	pomieszczenie socjalne	- pomieszczenie zamykane drzwiami na klucz; - drzwi balkonowe antywłamaniowe; - alarm; - grupa interwencyjna – Konsalnet;
3.	Długobórz, ul. Zambrowska 5 18-300 Zambrów	Biuro	- drzwi wejściowe zamykane na klucz; -alarm; - grupa interwencyjna – Konsalnet; - metalowa szafa ognioodporna z zamkiem szyfrowym;
4.	ul. Długa 50 18-312 Rutki-Kossaki	Recepcja	- drzwi wejściowe zamykane na klucz; - podwójne drzwi wewnętrzne zamykane na klucz; - pomieszczenie z półkami na dokumenty zamykane na klucz; - kraty antywłamaniowe w oknach;
5.	al. Wojska Polskiego 3 18-300 Zambrów	Recepcja	- drzwi wejściowe antywłamaniowe zamykane na klucz - kraty i rolety antywłamaniowe w oknach; - szafka zamykana na klucz; - alarm

§5
Obowiązek informacyjny

Zgodnie z art. 13 ust. 1 i 2 RODO Administrator Danych Osobowych spełnia obowiązek w momencie zbierania danych osoby, przekazując jej wymagane informacje poprzez:

1) udostępnienie wymaganych informacji na swojej stronie internetowej oraz w siedzibie firmy w ogólnodostępnym miejscu;
2) umieszczenie klauzuli informacyjnej na pisemnej zgodzie na przetwarzanie danych osobowych oraz na fakturach;
3) wysyłanie klauzuli informacyjnej w odpowiedzi na przychodzące mailowo CV;
4) umieszczenie klauzuli informacyjnej w dokumentach przy zatrudnianiu;
5) wysłanie niezbędnych informacji przy pomocy sms;
6) zobowiązanie pracowników w regulaminie pracy do przekazywania niezbędnych informacji klientom przed wykonaniem usługi.

§6
Bezpieczeństwo przetwarzania i zgłaszanie naruszeń

1. Administrator Danych Osobowych zgodnie z art. 32 RODO zapewnia bezpieczeństwo przetwarzania danych gwarantując:
   1) jeśli zajdzie konieczność pseudonimizację lub szyfrowanie danych przy pomocy dostępnych programów;
   2) w celu zachowania ciągłej zdolności do zapewnienia bezpieczeństwa regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych zgodnie z planem sprawdzeń (*zał. 10*), nie rzadziej niż raz do roku, zwieńczone sprawozdaniem, którego wzór stanowi *zał. 11*;
   3) wprowadza do stosowania Instrukcję Zarządzania Systemem Informatycznym, która stanowi *zał. 12;*
   4) monitoruje przetwarzanie danych osobowych przez podmioty przetwarzające;
   5) nadanie upoważnienia wszystkim pracownikom stosownie do wykonywanych obowiązków, którego wzór stanowi *zał. 13*;
   6) szkolenie nowo przybyłych pracowników z zakresu ochrony danych osobowych w podmiocie oraz cykliczne szkolenia obecnych pracowników nie rzadziej niż raz na dwa lata zwieńczone zaświadczeniem, którego wzór stanowi *zał. 14*, wraz z prowadzeniem rejestru osób przeszkolonych – *zał. 15*;
   7) każdy pracownik podpisuje umowę poufności, której wzór stanowi *zał. 16* wraz z prowadzeniem rejestru osób, które podpisały umowę – *zał. 17*;
   8) każdy praktykant przechodzi wstępne przeszkolenie w zakresie ochrony danych osobowych, podpisuje klauzulę poufności (*zał. 18*) i przebywa w obszarze przetwarzania danych osobowych wyłącznie w obecności osób upoważnionych.
2. Administrator Danych Osobowych w ślad za art. 33 RODO, jeśli odnotuje naruszenie ochrony danych osobowych skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych, zgłasza ten fakt organowi nadzorczemu właściwemu zgodnie z art. 55 bez zbędnej zwłoki, w miarę możliwości w terminie do 72 godzin po jego stwierdzeniu. Jeśli przekroczy ten termin jest obowiązany do złożenia wyjaśnień. Wzór zgłoszenia stanowi *zał. 19*.
3. Jeśli naruszenie nie skutkuje naruszeniem praw lub wolności osób fizycznych, Administrator nie dokonuje zgłoszenia, ale zgodnie z art. 33 ust. 5 RODO musi je udokumentować. Wzór dokumentacji stanowi *zał. 20.*

§7
Respektowanie praw osób, których dane dotyczą

1. Administrator Danych Osobowych zobowiązuje się do respektowania praw osób, których dane dotyczą i umożliwia korzystanie z nich poprzez:
   1) na wniosek osoby, której dane dotyczą, nie później jak w ciągu 30 dni od jego złożenia, udziela dostępu do jej danych poprzez przekazanie kopii przetwarzanych

danych oraz wszystkich dodatkowych informacji wymaganych w art. 15 ust. 1 RODO;

2) na wniosek osoby, której dane dotyczą, dokonuje niezwłocznego sprostowania nieprawidłowych danych dotyczących tejże;
3) na wniosek osoby, której dane dotyczą, dokonuje niezwłocznego usunięcia/anonimizacji jej danych, jeżeli zachodzi jedna z okoliczności wymienionych w art. 17 ust. 1 lit. a)-f) RODO;
4) na wniosek osoby, której dane dotyczą, ogranicza przetwarzanie danych tejże poprzez jego zaprzestanie w przypadkach wymienionych w art. 18 ust. 1 lit a)-d) RODO
5) na wniosek osoby, której dane dotyczą, przekazuje jej kopię danych osobowych drogą mailową w formacie umożliwiającym edycję bądź przekazuje te dane innemu administratorowi wskazanemu przez tę osobę;
6) w przypadku danych osoby uzyskanych na podstawie zgody, Administrator w momencie zgłoszenia sprzeciwu, wycofania zgody, zaprzestaje ich przetwarzania.

§8
Przepisy końcowe

1. Polityka ma zastosowanie do wszystkich komórek organizacyjnych w tym: oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych
2. W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.*

Podpis Administratora Danych Osobowych

……