PRZYCHODNIA WETERYNARYJNA

"VETMEDICOR" S.C.

TARNOWSKIE GÓRY

UL. SIENKIEWICZA 36

POLITYKA BEZPIECZEŃSTWA

Data i miejsce sporządzenia dokumentu:	22/05/2018
Ilość stron:	34

SPIS TREŚCI

1. WSTĘP

1.1. INFORMACJE OGÓLNE

1. Wskazanie Administratora Danych, który wdraża Politykę Bezpieczeństwa.

1.1. Administratorem danych osobowych który wdraża Politykę Bezpieczeństwa jest Marcin Kukla

2. Wyjaśnienie celu wprowadzania dokumentu.

2.1. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania ADMINISTRATORA DANYCH z Ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi.

3. Wskazanie podstaw prawnych.

3.1. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 ze zm.),

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.).

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

1.2. Dane osobowe zbierane są, przetwarzane i archiwizowane w siedzibie firmy przy ulicy Sienkiewicza 36 w Tarnowskich Górach

1.3. Dane przetwarzane są na wszystkich pomieszczeniach w firmie

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

2.2. Dane osobowe w zbiorze przetwarzane są przy użyciu programu Klinika XP zainstalowanego na komputerze mieszczącym się w gabinecie przyjęć.

2.3. W zbiorze przetwarzane są następujące dane osobowe: imię, nazwisko, adres zamieszkania, e-mail, numer telefonu oraz nip i nazwa firmy (dotyczy firm i fundacji)

2.4. Dane przechowywane są w bazie danych aplikacji: KlinikaXp

2.5. Kopia bazy danych przechowywana jest lokalnie na komputerach znajdujących się w firmie

2.6. Dane przetwarzane są w obrębie jednej aplikacji: KlinikaXp

3. Komputery na których przetwarzane są dane osobowe zabezpieczono w następujący sposób:

3.2. Zainstalowano oprogramowanie antywirusowe oraz ustawiono firewall

3.3. Dostęp do sieci WiFi w której pracują komputery został zabezpieczony hasłem (hasło składa się przynajmniej z 8 znaków, w tym przynajmniej 1 dużej litery, 1 cyfry); hasło zmieniane jest co 30 dni

3.4. Komputery zabezpieczono hasłem (hasło składa się przynajmniej z 8 znaków, w tym przynajmniej 1 dużej litery, 1 cyfry); hasło zmieniane jest co 30 dni

3.5. Dostęp do programu w którym dane są przetwarzane został zabezpieczony hasłem (hasło składa się przynajmniej z 8 znaków, w tym przynajmniej 1 dużej litery, 1 cyfry); hasło zmieniane jest co 30 dni

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1. **Administrator danych** – organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 Ustawy o ochronie danych osobowych, decydująca o celach i środkach przetwarzania danych osobowych,
2. **ABI** – Administrator Bezpieczeństwa Informacji,
3. **ASI** – Administrator Systemów Informatycznych,
4. **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.),

5. **rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

1. Administrator danych – Przychodnia Weterynaryjna "Vetmedicor" s.c.42-600 Tarnowskie Góry ul. Sienkiewicza 36 , NIP 645 00 07 301

2.2. ADMINISTRATOR DANYCH

1. Administratorem danych osobowych jest Przychodnia weterynaryjna "Vetmedicor" s.c. ul.Sienkiewicza 36, 42-600 Tarnowskie Góry NIP 645 00 07 301

2.3. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.

2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Kto nadaje upoważnienie – Janusz Kirsz
2. Na czyj wniosek upoważnienie jest nadawane – na wniosek pracownika lub osoby zatrudnionej w ramach kontraktu.
3. Forma wniosku – pisemna – załącznik do dokumentu
4. Forma upoważnienia – pisemna – załącznik do dokumentu
5. Forma zapoznania osoby upoważnionej z zasadami ochrony danych osobowych – szkolenie przeprowadzane przez Administratora danych.
6. Kto ostatecznie decyduje i ponosi odpowiedzialność za nadanie upoważnienia – Administrator danych
7. Kto ewidencjonuje nadane upoważnienia – Administrator danych.
8. Forma prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych – lista załączona do dokumentu
9. Wzór upoważnienia stanowi Załącznik nr 4a i 4b Polityki Bezpieczeństwa.
10. Wzór ewidencji osób upoważnionych do przetwarzania danych stanowi Załącznik nr 7 do Polityki Bezpieczeństwa.

4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe przetwarzane są tylko przez Przychodnię Weterynaryjną "Vetmedicor", 42-600 Tarnowskie Góry NIP 645 00 07 301 i nie są udostępniane firmom zewnętrznym

5. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
2. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
3. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
4. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
5. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
7. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

6. INSTRUKCJA POSTĘPOWNIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Danych.
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Danych lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:
    - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
    - zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
    - udokumentować wstępnie zaistniałe naruszenie,
    - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Danych lub osoby upoważnionej.
3. Po przybyciu na miejsce naruszenia ochrony danych osobowych, Administrator Danych lub osoba go zastępująca:
    - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania
    - wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
4. Administrator Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport według wzoru stanowiącego Załącznik nr 2 do niniejszej Instrukcji.

   Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Danych zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

7. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Przychodni Weterynaryjnej "Vetmedicor" s.c., 42-600 Tarnowskie Góry NIP 645 00 07 301 sprawuje Administrator Danych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.

8. OPIS STRUKTURY ZBIORÓW DANYCH

Nr	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Rodzaj danych				
						imię	nazwisko	adres	email	telefon
1.	Klinika XP	Klinika XP	Zbieranie, przechowywanie i archiwizowanie	Administrator danych i osoby upoważnione	Wszelkie czynności związane z przetwarzaniem	x	x	x		
2.	wetsystem	Internetowy rejestr paszportów	Ewidencja paszportowa	Administrator danych i osoby upoważnione	Wszelkie czynności związane z przetwarzaniem	x	x	x		x
3.	Safeanimal	Internetowy rejestr mikroczipów	Rejestracja zaczipowanych zwierząt	Administrator danych i osoby upoważnione	Wszelkie czynności związane z przetwarzaniem	x	x	x		x
4.	Wojewódzki inspektorat weterynaryjny	Informacja przesyłana drogą mailową	Ustawowy obowiązek zgłaszania zaszczepionych zwierząt przeciwko wściekliźnie	Administrator danych i osoby upoważnione	Wszelkie czynności związane z przetwarzaniem	x	x	x		
5.	IDEXX	Skierowanie na badanie	Wykonanie oznaczeń w laboratorium	Administrator danych i osoby upoważnione	Wszelkie czynności związane z przetwarzaniem	x	x			
6.	WetLab	Skierowanie na badanie	Wykonanie oznaczeń w laboratorium	Administrator danych i osoby upoważnione	Wszelkie czynności związane z przetwarzaniem	x	x			
7	Laboklin	Skierowanie na badanie	Wykonanie oznaczeń w laboratorium	Administrator danych i osoby upoważnione	Wszelkie czynności związane z przetwarzaniem	x	x			

8	Nadzór farmaceutyczny	Książka kontroli środków odurzających i psychotropowych	Ewidencja użycia leków wynikająca z ustawy	Administrator danych i osoby upoważnione	Wszelkie czynności związane z przetwarzaniem	x	x			
9										
10										

9. OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Określenie obszaru pomieszczeń, w których przetwarzane są dane osobowe, powinno obejmować zarówno miejsca, w którym wykonuje się operacje na danych osobowych (2 x pomieszczenia biurowe i 2 2x gabinety weterynaryjne przychodni, laboratorium), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe.(biuro , pokój - archiwum)

2. Wskazując na obszar przetwarzania danych należy uwzględnić także obszar, w którym przetwarzane są dane powierzone przez Administratora Danych odrębnym podmiotom.

Wykaz podmiotów, którym dane zostały powierzone, wraz ze wskazaniem obszaru przetwarzania danych znajduje się w Załączniku nr 8 do Polityki Bezpieczeństwa.

	Administrator Danych	Uwagi
Dane osobowe przetwarzane jako Administrator Danych	Janusz Kirsz	Dane przetwarzane przy użyciu programu KlinikaXP który zainstalowany jest na komputerach w firmie.
Dane osobowe przetwarzane jako osoba upoważniona	Łukasz Łebek ,Barbara Gruca, Bartłomiej Topór , Andrzej Kirsz, Wiesław Topór , Jadwiga Kirsz	Dane przetwarzane przy użyciu programu Klinika XP który zainstalowany jest na komputerach w firmie.

10. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

Środek ochrony fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi** (niewzmacnianymi, nie przeciwpożarowymi).	TAK	
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za **pomocą rolet**	TAK	
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w **system alarmowy przeciwwłamaniowy.**	TAK	
4. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są **systemem kontroli dostępu.**	TAK	
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**	NIE	
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych** tam pracowników **nadzorowany przez służbę ochrony.**	NIE	
7. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej **niemetalowej szafie w osobnym pomieszczeniu**	TAK	
8. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie w osobnym pomieszczeniu**	TAK	

9. Zbiór danych osobowych w formie papierowej przechowywany jest **w zamkniętym sejfie lub kasie pancernej.**	TAK	
10. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**	TAK	
11. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w osobnym zamkniętym pomieszczeniu**.	NIE	
12. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą **systemu przeciwpożarowego** i/lub **wolnostojącej gaśnicy.**	TAK	
13. Dokumenty zawierające dane osobowe **po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.**	TAK	

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	Zastosowano (TAK / NIE)	Uwagi
Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	TAK	
Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.	TAK	
Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	TAK	
Użyto system Kacperky do ochrony dostępu do sieci komputerowej.	TAK	

Środek organizacyjny	Zastosowano (TAK / NIE)	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych	**TAK**	

Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych	**TAK**	
Powołano Administratora Bezpieczeństwa Informacji	**TAK**	
Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych	**TAK**	
Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych	**TAK**	
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych	**TAK**	
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	**TAK**	
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy	**TAK**	
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym	**TAK**	
Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco	**TAK**	

11. ZAŁĄCZNIKI

Załącznik nr 1 – Powołanie Administratora Bezpieczeństwa Informacji

Załącznik nr 2 – Upoważnienie Administratora Bezpieczeństwa Informacji do nadawania upoważnień

Załącznik nr 3 – Wyznaczenie Administratora Systemów Informatycznych

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie innej umowy niż umowa o pracę

Załącznik nr 5 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

Załącznik nr 6 – Opis struktury zbiorów danych

Załącznik nr 7 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 8 – Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych

Załącznik nr 9 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Załącznik nr 10 –Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

Załącznik nr 11 – Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających

Dokument sporządzono:	**Pełen podpis Administratora Danych:**	**Pieczęć**
Data: 25.05.2018 Miejsce: ……		

Załącznik nr 1 – Ustanowienie Administratora Bezpieczeństwa Informacji

Niniejszym, na podstawie art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm. dalej: „Ustawa") oraz reprezentując Administratora danych Przychodnię Weterynaryjną "Vetmedicor" s.c. 42-600 Tarnowskie Góry ul. Sienkiewicza 36 NIP 645 00 0 7 301 **powołuję**Pana ……..

na stanowisko **Administratora Bezpieczeństwa Informacji (ABI)** w Przychodni Weterynaryjnej "Vetmedicor" s,c, 42-600 Tarnowskie Góry ul. Sienkiewicza 36

Jednocześnie, na podstawie art. 37 Ustawy upoważniam Pana ……. do przetwarzania danych osobowych we wszystkich zbiorach Administratora Danych w zakresie niezbędnym dla należytego wykonywania funkcji Administratora Bezpieczeństwa Informacji.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Bezpieczeństwa Informacji określone są Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 roku oraz dokumentacją z zakresu ochrony danych osobowych (Polityką Bezpieczeństwa i Instrukcją zarządzania systemem informatycznym) wdrożoną dnia 25…/ 05… / 2018…… (dd/mm/rrrr) w NAZWA ADMINISTRATORA DANYCH.

DATA I PODPIS OSOBY POWOŁANEJ NA STANOWISKO ABI	DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

Załącznik nr 2 – Upoważnienie Administratora Bezpieczeństwa Informacji do nadawania upoważnień

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych – Przychodni Weterynaryjnej 'Vetmedicor"s.c., 42-600 NIP 645 00 07 3017

upoważniam

Pana …Janusza Kirsz – **Administratora Bezpieczeństwa Informacji** w Przychodni weterynaryjnej "Vetmedicor" s.c. do nadawania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych.

DATA I PODPIS OSOBY POWOŁANEJ NA STANOWISKO ABI	DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

Załącznik nr 3 – Wyznaczenie Administratora Systemów Informatycznych

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych Przychodni Weterynaryjnej "Vetmedicor" s.c., 42-600 Tarnowskie Góry NIP 645 00 07 301

wyznaczam Pana ……..

na stanowisko **Administratora Systemów Informatycznych** w Przychodni Weterynaryjnej "Vetmedicor" s.c., 42-600 Tarnowskie Góry NIP 645 00 07 301

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone są dokumentacją ochrony danych osobowych (Polityką Bezpieczeństwa i Instrukcją zarządzania systemem informatycznym) wdrożoną dnia 25.05..2018 w Przychodni Weterynaryjnej "Vetmedicor" s.c., 42-600 Tarnowskich Górach NIP 645 00 07 301

DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO ASI	DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Bezpieczeństwa Informacji w Przychodni Weterynaryjnej "Vetmedicor", 42-600 Tarnowskich Górach NIP 645 00 07 301, na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 ze zm.), **upoważniam:**

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	**Dane osobowe klientów i pracowników**

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 ze zm.), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Dogtor Miau I.Stepańczak-Opydo J.Kukla s.c. Grunwaldzka 215, 43-600 Jaworzno NIP 6322011047wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania.

....

Data i podpis upoważniającego Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Przychodni Weterynaryjnej "Vetmedicor" s.c., 42-600 Tarnowskie Góry NIP 6450007301 (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie innej niż umowa o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Bezpieczeństwa Informacji w Przychodni Weterynaryjnej "Vetmedicor" s.c., 42-600 Tarnowskich Górach NIP 645 00 07 301), na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 ze zm.), **upoważniam:**

Imię i nazwisko upoważnionego	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 ze zm.), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Przychodni Weterynaryjnej "Vetmedicor" s.c., 42-600 Tarnowskie Góry NIP 64500 0703017wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz odpowiedzialności cywilnej.

Upoważnienie jest ważne do odwołania.

....

Data i podpis upoważniającego Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Przychodni Weterynaryjnej "Vetmedicor" s.c., 42-600 Tarnowskie Góry NIP 645 00 07 301 (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych w związku z pełnioną przeze mnie funkcją i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu stosunku prawnego łączącego mnie z Administratorem Danych.

……..……..

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Załącznik nr 5 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

Tarnowskie Góry , dnia 25.05.2018 r.

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y . . . . zamieszkała/y w . . . . zatrudniona/y na stanowisku . . . . zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z …………………………….. Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

……………………………….……………………..

Podpis

Załącznik nr 6 – Opis struktury zbiorów danych

Nr	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
1.	FAKTURY	KLINIKA XP	Wystawianie faktur	Klient- właściciel zwierzęcia	Nazwisko i imię lub nazwa firmy , adres NIP (dla firm)	
2.	ZUS	Biuro rachunkowe "DEBET"	Obowiązek pracodawcy	Pracodawcy i pracownicy	Dane osobowe niezbędne do przetwarzania wynikające ze stosunku pracy	
2.	PODATKI	Biuro rachunkowe "DEBET"	Obowiązek pracodawcy	Pracodawcy i pracownicy	Dane osobowe niezbędne do przetworzenia wynikające ze stosunku pracy	
3.	LABORATORIUM	Aparatura medyczna RTG, aparaty do biochemii i morfologii	Niezbędne do identyfikacji	Klient-właściciel zwierzęcia	Nazwisko i imię	
4.	ZBIÓR KART INFORMACYJNYCH	W formie papierowej	Zgodne z wymaganiami Nadzoru Farmaceuty-cznego	Klient-właściciel zwierzęcia	Nazwisko i imię , adres zamieszkania	
5.						

6.						
7.						
8.						
9.						

Załącznik nr 7 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator w systemie informatycznym	Nazwy zbiorów objętych zakresem upoważnienia
1.	JADWIGA KIRSZ	22.05.2018		1/2018	KLIENCI, ZUS , PODATKI, SPRAWY FIRMY
2.	LUKASZ LEBEK	22.05.2018		2/2018	KLIENCI
3.	BARBARA GRUCA	22.05.2018		3/2018	KLIENCI
4.	BARTŁOMIEJ TOPÓR	22.05.2018		4/2018	KLIENCI
5.	ANDRZEJ KIRSZ	22.05.2018		5/2018	KLIENCI , ZUS , PODATKI ,SPRAWY FIRMY
6.	WIESŁAW TOPÓR	22.05.2018		6/2018	KLIENCI , ZUS, PODATKI ,SPRAWY FIRMY
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

Załącznik nr 8 – Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych

	Adres / lokalizacja	Uwagi
Podmioty, którym Administrator Danych powierzył przetwarzanie danych osobowych	**DEBET SP. Z O.O. UL. GLIWICKA 35 42-600 TARNOWSKIE GÓRY ZUS, URZĄD SKARBOWY**	
	IZBA LEKARSKO - WETERYNARYJNA W KATOWICACH UL. WALECZNYCH 4, SAFE ANIMAL -BAZA IDENTYFIKACJI ZWIERZĄT	

Załącznik nr 9 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

ŚRODKI FIZYCZNE

* **Przykładowe środki fizyczne**

Środek ochrony fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi** (niewzmacnianymi, nie przeciwpożarowymi).	TAK	
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za **pomocą krat, rolet lub folii antywłamaniowej.**	TAK	
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w **system alarmowy przeciwwłamaniowy.**	TAK	
4. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są **systemem kontroli dostępu.**	TAK	
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**	NIE	
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych** tam pracowników **nadzorowany przez służbę ochrony.**	NIE	
7. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej **niemetalowej szafie.**	TAK	
8. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie.**	TAK	
9. Zbiór danych osobowych w formie papierowej przechowywany jest **w zamkniętym sejfie lub kasie pancernej.**	TAK	

10. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**	TAK	
11. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w zamkniętej metalowej szafie**.	TAK	
12. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą **systemu przeciwpożarowego** i/lub **wolnostojącej gaśnicy.**	TAK	
13. Dokumenty zawierające dane osobowe **po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.**	TAK	

ŚRODKI TECHNICZNE

Przykładowe środki techniczne

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	Zastosowano (TAK / NIE)	Uwagi
Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	TAK	
Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.	TAK	
Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	TAK	
Użyto system Kaspersky do ochrony dostępu do sieci komputerowej.	TAK	

ŚRODKI ORGANIZACYJNE

Przykładowe środki organizacyjne

Środek organizacyjny	Zastosowano (TAK / NIE)	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych	**TAK**	
Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych	**TAK**	
Powołano Administratora Bezpieczeństwa Informacji	**TAK**	
Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych	**TAK**	
Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych	**TAK**	
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych	**TAK**	
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	**TAK**	
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy	**TAK**	
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym	**TAK**	
Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco	**TAK**	

Załącznik nr 10 - Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

Tarnowskie Góry

…25.05.2018……

……..

miejscowość, data

SPRAWOZDANIE

ZE SPRAWDZENIA ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

z przepisami o ochronie danych osobowych

1. Administrator Danych: …….....
2. Administrator Bezpieczeństwa Informacji: ……
3. Wykaz czynności podjętych w toku sprawdzenia: ……

   ……

   ……

   ……

   ……
4. Data rozpoczęcia sprawdzenia: …….....
5. Data zakończenia sprawdzenia: …….....
6. Przedmiot i zakres sprawdzenia: …….....

   ……

   ……

   ……

   ……
7. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych: ……

   ……

   ……

   ……

   ……

8. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem: …..

   ……
   ……
   ……
   ……
   ……
   ……
   ……
   ……

9. Załączniki:

.....

Podpis ABI

Załącznik nr 11 - Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/ czynności sprawdzających ……..

Tarnowskie Góry 25.05.2018 r. miejscowość, data

PROTOKÓŁ

Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*

w zakresie ochrony danych osobowych

10. Nazwa kontrolowanej jednostki organizacyjnej:…….....
11. Zbiory danych osobowych, których przetwarzanie podlega kontroli: …….....
12. Data wykonania czynności kontrolnych:…….....
13. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne: …….....
14. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej:……..……..…… ….....…..……..

6. Ustalenia dokonane w trakcie czynności kontrolnych:……
   ……
   ……
   ……
   ……
   ……
   ……
7. Wnioski i zalecenia pokontrolne:
   ……
   ……
   ……
   ……
   ……
   ……

…….. ……...

(data i podpis osoby wykonującej czynności kontrolne) (data i podpis kierownika kontrolowanej kom. organizacyjnej)

Otrzymują:
1 x Kierownik kontrolowanej jednostki organizacyjnej
1 x Administrator Bezpieczeństwa Informacji

* niepotrzebne skreślić