INSTRUKCJA ZARZĄDZANIA
SYSTEMAMI INFORMATYCZNYMI
PRZETWARZAJĄCYMI DANE OSOBOWE
W
PRO-BET SP.J.
OLEWIN 50 C, 32 - 300 OLKUSZ
KRS: 0000250867

21.06.2018 r., Kraków
[Data i miejsce sporządzenia dokumentu]

13 (trzynaście)
[Ilość stron]

Spis treści

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI PRZETWARZAJĄCYMI DANE OSOBOWE W SPÓŁCE PRO - BET SP. J.

Definicje:

1. Administrator Danych Osobowych - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych
2. Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych
3. Identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie
4. Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie
5. Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
6. System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych
7. Użytkownik - osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych
8. Zbiór danych - każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów
9. Uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

I. WSTĘP DO DOKUMENTU INSTRUKCJI ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI PRZETWARZAJĄCYMI DANE OSOBOWE

1. Administratorem Danych Osobowych jest spółka Przedsiębiorstwo Produkcyjno – Handlowo – Usługowe „Pro-Bet" Spółka Jawna Stanisław Babiuch, Jarosław Majda z siedzibą w Olkuszu (32-300), Olewin 50C, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia w Krakowie, XII Wydział Gospodarczy KRS pod numerem 0000250867, posiadająca nr NIP 6371575407, REGON 273418363.

2. Niniejsza Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych spółki Pro-Bet Sp.j. przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z Ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych, w tym z zasadą art. 5 ust. 2 rozporządzenia Parlamentu

Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwane dalej RODO.

3. Zasadniczym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa tych danych. Priorytetowe jest zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemów informatycznych stosowanych w Pro-Bet Sp.j.

4. Istotnym elementem osiągnięcia celu, o którym mowa w pkt. 3 powyżej jest zapewnienie odpowiedniego poziomu oraz kontroli dostępu:
a) do sieci, w tym urządzeń serwerowych;
b) do systemów operacyjnych;
c) do aplikacji;
d) do informacji i zbiorów danych, wraz z określeniem trybu dostępu.

5. Niniejsza Instrukcja została opracowana zgodnie z wymogami określonymi w § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. Nr 100, poz. 1024), zwane dalej Rozporządzeniem.

II. DOKUMENTY POWIĄZANE

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Pro-Bet Sp.j. wraz z załącznikami stanowiącymi jej integralną część.

III. KONFIGURACJA SPRZĘTU KOMPUTEROWEGO UŻYTKOWNIKA SYSTEMU

1. Systemy informatyczne służące do przetwarzania danych osobowych należy chronić przed niebezpieczeństwami pochodzącymi z sieci publicznej poprzez wprowadzenie fizycznych oraz logicznych zabezpieczeń chroniących przed nieupoważnionym dostępem, w tym kontroli przepływu informacji pomiędzy systemami a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemów.

2. Każdy dostęp do danych osobowych, musi być zarejestrowany.

3.Wszystkie urządzenie mobilne zawierające dane osobowe muszą być odpowiednio zabezpieczone przed nieupoważnionym dostępem poprzez wykorzystanie szyfrowania dysku twardego lub inny sposób szyfrowania i ochrony dostępu do danych.

4. Minimalne środki ochrony to:
a) zainstalowanie na stacjach zapory sieciowej firewall i oprogramowania antywirusowego;
b) wdrożenie systemu aktualizacji systemu operacyjnego oraz jego składników;

c) wymaganie podania hasła przed uzyskaniem dostępu do systemu operacyjnego;
d) niepozostawianie niezablokowanych stacji roboczej bez nadzoru.

IV. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH

1. Do obsługi systemów informatycznych oraz urządzeń wchodzących w ich skład, służących do przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych Osobowych.

2. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany identyfikator użytkownika. Z chwilą nadania identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.

3. Dla każdego użytkownika systemu informatycznego ustalony jest odrębny identyfikator i hasło.

4. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.

5. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, zostaje niezwłocznie wyrejestrowany z systemu informatycznego, w którym są przetwarzane, zaś hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

6. Każda osoba dopuszczona do pracy przy przetwarzaniu danych osobowych:
   a) weryfikuje poprawność jej konta i ustawień oraz otrzymuje zakres czynności określający jej uprawnienia i odpowiedzialność;
   b) otrzymuje od Administratora Danych Osobowych upoważnienie w formie pisemnej do przetwarzania danych, potwierdza własnoręcznym podpisem znajomość dokumentów warunkujących dostęp do przetwarzanych danych osobowych oraz zobowiązanie do przetwarzania danych osobowych zgodnie z prawem na podstawie oświadczenia;
   c) zostaje umieszczona w ewidencji osób mających dostęp i upoważnionych do przetwarzania danych osobowych;
   d) w przypadku zniszczenia, utraty, udostępnienia danych z powierzonego jej zakresu, ponosi odpowiedzialność określoną w Rozporządzeniu.

7. Zarejestrowania i wyrejestrowania użytkowników systemów informatycznych służących do przetwarzania danych osobowych dokonują osoby wyznaczone i upoważnione przez Administratora Dancych Osobowych.

V. METODY I ŚRODKI UWIERZYTELNIENIA W SYSTEMACH INFORMATYCZNYCH

1. Do pracy z systemami informatycznymi przetwarzającymi dane osobowe dopuszczani są jedynie użytkownicy posiadający indywidualny identyfikator użytkownika i osobiste hasło.

2. Hasła użytkowników umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.

3. Zabrania się używania identyfikatora lub hasła drugiej osoby.

4. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu,
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
   c) informacji o odbiorcach, którym dane osobowe zostały udostępnione.

5. Zmiana haseł użytkowników do systemów informatycznych przetwarzających dane osobowe jest wymuszana nie rzadziej niż co 30 dni.

6. Każdy użytkownik, który otrzyma identyfikator i hasło, jest zobowiązany do niezwłocznej zmiany tego hasła przy pierwszym logowaniu, w taki sposób, aby było ono znane jedynie użytkownikowi.

7. Hasło Użytkownika:
   a) musi się składać co najmniej z 8 znaków, w tym zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
   b) nie może zawierać znaków następujących po sobie na klawiaturze bądź tych samych liter lub cyfr;
   c) nie może zawierać imion, nazwisk, przezwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów i innych kombinacji znaków mogących doprowadzić do łatwego rozszyfrowania go przez osoby nieupoważnione;
   d) nie może być zapisywane w systemie w postaci jawnej;
   e) nie może być wyświetlane na ekranie komputera w sposób jawny;
   f) nie może być ujawnione innej osobie, nawet po utracie ważności;
   g) musi być zabezpieczone przez użytkownika przed nieuprawnionym dostępem osób trzecich.

8. Prawidłowa konstrukcja i terminowa zmiana haseł jest obowiązkiem każdej osoby przetwarzającej dane.

9. Bezwzględnie zabrania się:
   a) udostępniania osobom trzecim swoich loginów i haseł;
   b) udostępniania osobom trzecim swoich loginów i haseł do poczty elektronicznej;
   c) wykonywania pracy przy wykorzystaniu konta innej osoby;

d) wszelkich działań, które mogą zagrozić stabilności sieci komputerowej lub pracy pojedynczych urządzeń komputerowych;
e) instalacji i uruchamiania oprogramowania nieautoryzowanego.

10. Sposoby realizacji wymogu zapisania w systemie informatycznym informacji o odbiorcach danych:
a) informacje o odbiorcach danych zapisywane są w systemie informatycznym, z którego nastąpiło udostępnienie;
b) informacja o odbiorcy danych zapisana jest w systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych;
c) możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

VI. ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY PRZEZ UŻYTKOWNIKÓW SYSTEMÓW

1. Każdy użytkownik po przyjściu do pracy uruchamia stację roboczą.

2. Każdy użytkownik, przed rozpoczęciem pracy, ma obowiązek każdorazowo sprawdzić, czy nie został naruszony stan bezpieczeństwa fizycznego poprzez sprawdzenie okien, rolet, drzwi do pomieszczenia.

3. W wypadku, gdy istnieje podejrzenie naruszenia integralności sprzętu, sieci, bądź nieprawidłowego funkcjonowania systemu informatycznego, użytkownik powiadamia przełożonego, który wspólnie z Administratorem Danych Osobowych podejmuje odpowiednie kroki.

4. W celu zalogowania do systemu informatycznego, użytkownik wprowadza swój identyfikator oraz hasło w sposób uniemożliwiający zapoznanie się z nimi osobom postronnym.

5. W przypadku 5-krotnego wprowadzenia błędnych danych (login, hasło), dostęp zostanie zablokowany na 10 minut. Po upływie 10 minut, użytkownik może ponownie podjąć czynności zalogowania się. W przypadku nieodblokowania systemu, należy niezwłocznie zawiadomić Administratora Danych Osobowych.

6. Przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby osoby postronne nie miały dostępu do danych przetwarzanych na tym stanowisku.

7. Każdy użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem oraz wylogowania się z systemu lub jego blokowania.

8. Zablokowanie komputera odbywa się poprzez naciśnięcie kombinacji klawiszy.

9. Niezależnie od powyższego, wygaszacz ekranu aktywuje się nie później niż w 10 minucie bezczynności użytkownika.

10. Odblokowanie odbywa się poprzez ponowne zalogowanie się tego samego użytkownika.

11. W przypadku zawieszenia pracy w systemie informatycznym z powodu potrzeby załatwienia sprawy z osobą postronną znajdującą się w tym samym pomieszczeniu, użytkownik ma obowiązek zabezpieczenia ekranu komputera lub urządzenia mobilnego oraz dokumentów i wydruków znajdujących się na biurku w sposób uniemożliwiający podgląd zawartych w nich treści.

12. Po zakończeniu pracy z systemem, użytkownik jest zobowiązany do wylogowania się oraz do wyłączenia komputera.

13. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików. Użytkownik powinien pozostać przy komputerze do chwili ich zamknięcia.

14. Użytkownik kończący pracę powinien sprawdzić, czy wszystkie elektroniczne nośniki informacji lub wydruki i dokumenty zawierające dane osobowe zostały zabezpieczone przed dostępem osób nieuprawnionych.

15. Po zakończonym dniu pracy, ostatnia opuszczająca pomieszczenie osoba ma obowiązek sprawdzenia wyłączenia zbędnych urządzeń elektrycznych i łączności, sprawdzenia zamknięcia okien, rolet oraz drzwi.

VII. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

2. Za tworzenie i przechowywanie kopii zapasowych, o których mowa w ust. 1, w sposób zgodny z przepisami oraz niniejszą Instrukcją odpowiedzialny jest Administrator Danych Osobowych.

3. Dostęp do kopii zapasowych posiada wyłącznie Administrator Danych Osobowych lub w wyjątkowych wypadkach, osoba przez niego upoważniona.

VIII. PRZECHOWYWANIE NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

1. Dane osobowe zapisane na elektronicznych nośnikach są przechowywane w szafach zamykanych na klucz, do których dostęp mają osoby upoważnione do przetwarzania danych osobowych. W przypadku, gdy przesłanki do przetwarzania tych danych ustaną, muszą zostać one usunięte w sposób uniemożliwiający ich odtworzenie. Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe, przechowywany jest w obszarze przetwarzania danych osobowych, w pomieszczeniach odpowiednio zabezpieczonych.

2. Dane osobowe, które są przekazywane poza obszar przetwarzania, muszą być odbierane za potwierdzeniem przez uprawnionych odbiorców, w sposób zapewniający zachowanie poufności danych.

3. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych używane na bieżąco.

4. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

IX. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA KOPII ZAPASOWYCH ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

1. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, a kopie awaryjne należy bezzwłocznie usuwać po ustaniu ich użyteczności w przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych.

2. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są przez okres, w którym istnieją przesłanki do ich przetwarzania. Po ustaniu przesłanek, o których mowa w zdaniu pierwszym, dane znajdujące się na kopiach zapasowych muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie.

X. BEZPIECZEŃSTWO ZASOBÓW INFORMATYCZNYCH

1. Reguły zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji, stanowiących tajemnicę służbową przed ich nieuprawnionym przetwarzaniem oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej.

2. Systemy informatyczne służące do przetwarzania danych osobowych, muszą posiadać certyfikat legalności i być na liście produktów serwisowanych przez producenta oprogramowania.

3. Systemy informatyczne są zabezpieczone przed utratą przetwarzanych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. Stosowane się listwy przepięciowe, UPS i baterie w urządzeniach przenośnych.

4. Każda osoba zatrudniona przy przetwarzaniu danych, w przypadku stwierdzenia naruszenia systemu ochrony danych osobowych musi niezwłocznie powiadomić o tym fakcie Administratora Danych Osobowych.

5. W celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej w serwerach, na których zainstalowana jest baza danych zawierająca dane osobowe, stosuje się macierz dyskową lub inne rozwiązanie wielodyskowe.

6. Jeśli Administrator Danych Osobowych wyraża zgodę na używanie komputerów przenośnych, użytkownik takiego komputera jest zobowiązany:

a) zachować szczególną ostrożność w użytkowaniu komputera zwłaszcza poza obszarem przetwarzania danych osobowych;
b) przechowywać dane osobowe w specjalnie szyfrowanych folderach lub partycjach;
c) zachować szczególną ostrożność korzystając z niezaufanych punktów dostępowych sieci Internet;
d) nigdy nie pozostawiać komputera w miejscach niezabezpieczonych przed nieupoważnionym dostępem osób trzecich;
e) użyć połączenia szyfrowanego do przesłania loginu i hasła w przypadku korzystania ze zdalnego dostępu do zasobów zawierających dane osobowe.

7. Systemy informatyczne muszą być chronione równolegle na wielu poziomach m.in. poprzez stosowanie oprogramowania antywirusowego, systemów typu firewall, odpowiednią konfigurację systemu aktualizacji systemu operacyjnego oraz realizację kopii bezpieczeństwa.

8. Oprogramowanie antywirusowe jest instalowane na wszystkich stanowiskach komputerowych oraz urządzeniach mobilnych i elektronicznych nośnikach informacji.

9. Aktualizacja oprogramowania antywirusowego odbywa się nie rzadziej niż raz w tygodniu, w sposób automatyczny dla wszystkich komputerów zainstalowanych w sieci.

10. Użytkownik na stanowisku komputerowym, importujący dane do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania.

11. O pojawiających się komunikatach wskazujących na wystąpienie zagrożenia spowodowanego szkodliwym oprogramowaniem, użytkownik jest zobowiązany niezwłocznie powiadomić Administratora Danych Osobowych.

12. Za wdrożenie, oraz aktualizację i korzystanie z oprogramowania odpowiada Administrator Danych Osobowych.

13. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.

14. Administrator Danych Osobowych może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora Danych Osobowych.

15. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem. W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

XI. SPOSOBY REALIZACJI W SYSTEMIE WYMOGÓW DOTYCZĄCYCH PRZETWARZANIA DANYCH (SPOSÓB REALIZACJI WYMOGU ZAPISANIA

W SYSTEMIE INFORMATYCZNYM INFORMACJI O ODBIORCACH DANYCH)

1. Informacja o odbiorcach danych zapisana jest w systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.

2. Możliwe jest sporządzenie i wydrukowanie, w zrozumiałej formie, raportu zawierającego powyższe informacje.

XII. PROCEDURA W PRZYPADKU STWIERDZENIA NARUSZENIA ZASAD BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

1. W przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń systemu informatycznego przez osoby nieuprawnione, jest on zobowiązany natychmiast poinformować o tym zajściu Administratora Danych Osobowych.

2. W przypadku wykrycia zagrożenia automatycznym działaniem, możliwe jest zablokowanie pracy w systemie do chwili podjęcia decyzji o sposobie postępowania.

3. W celu ograniczenia niebezpieczeństw dąży się, w miarę możliwości organizacyjnych, do maksymalnej unifikacji sprzętu, stosowanego oprogramowania, konfiguracji sprzętu i oprogramowania, a także rozwiązań organizacyjnych.

4. Administrator Danych Osobowych jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości - zgodnie z instrukcją postepowania wskazaną w Polityce Bezpieczeństwa Przetwatrzania Danych Osobowych w spółce Pro-Bet Sp.j.

5. Zaistniałe naruszenie powinno stać się przedmiotem szczegółowej, analizy z udziałem Administratora Danych Osobowych. Analiza powinna zawierać wszechstronna ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

XIII. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Nośniki zawierające dane osobowe powinny być wyraźnie oznaczone w sposób umożliwiający łatwą ich identyfikację, co ma na celu:
   a) uniknięcie przypadkowego udostępnienia ich do ponownego użycia;
   b) uniknięcie nieumyślnego ujawnienia danych osobowych;
   c) informowanie użytkowników o konieczności szczególnej ochrony tych nośników.

2. Ze względu na przeznaczenie dysków lub innych nośników elektronicznych do likwidacji, konserwacji lub przekazania podmiotom nieuprawnionym, stosuje się następujące kroki:

a) w przypadku likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
b) w przypadku przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
c) w przypadku naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie lub przeprowadza się ich serwis pod nadzorem Administratora Danych Osobowych.

3. Do wykonania przeglądów oraz konserwacji systemów i nośników informacji służących do przetwarzania danych, ma zastosowanie następująca procedura:
a) raz na 3 miesiące należy wykonać generalny przegląd systemu informatycznego, ustala poprawność działania wszystkich elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z Instrukcji zarządzania systemami IT.
b) jeśli zostaną stwierdzone nieprawidłowości w działaniu elementów systemu informatycznego podejmuje on działania mające na celu przywrócenie ich prawidłowego funkcjonowania.
c) kiedy zachodzi potrzeba wykorzystania podmiotu zewnętrznego do przywrócenia prawidłowego działania systemu, serwis taki jest wykonywany w obecności Administratora Danych Osobowych lub w szczególnych przypadkach, osoby przez niego wyznaczonej.

XIV. KOMUNIKACJA W SIECI KOMPUTEROWEJ

1. Jeżeli dane do systemu przetwarzającego dane osobowe dostępne są przez sieć publiczną, system do logowania użytkowników używa szyfrowania danych.

2. Organizacja sieci lokalnej jest skonstruowana w sposób, który pozwala użytkownikowi na dostęp do możliwie ograniczonych zasobów, niezbędnych mu do wykonania pracy.

3. Wydruki za pośrednictwem drukarki sieciowej lub drukarki w ogólnodostępnym pomieszczeniu, powinny być realizowane w taki sposób, aby zapobiec omyłkowemu, bądź celowemu odebraniu przez osoby niepowołane. Wydruk dokumentów o dużej objętości, powinien być nadzorowany bezpośrednio przez osobę realizującą.

XV. POSTANOWIENIA KOŃCOWE

1. Pro-Bet Sp.j. przetwarza dane osobowe na podstawie powszechnie obowiązujących przepisów prawa.

2. Niniejsza Instrukcji zarządzania systemami informatycznymi przetwarzającymi dane osobowe obowiązuje od dnia jej zatwierdzenia przez Administratora Danych Osobowych.

3. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, przepisów o ochronie danych osobowych.

4. W sprawach nieuregulowanych niniejszym dokumentem, zastosowanie mają Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych, Rozporządzenie Parlamentu Europejskiego

i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. Nr 100, poz. 1024).