WÓJT
Małgorzata Włodarczyk
Zatwierdzam:

Załącznik Nr 1
do Zarządzenia Nr 55/2015
Wójta Gminy Miasteczko Krajeńskie
z dnia 24 czerwca 2015 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH w Urzędzie Gminy Miasteczko Krajeńskie

OPRACOWAŁ:

Justyna Dziuba

Administrator Bezpieczeństwa Informacji

w Urzędzie Gminy Miasteczko Krajeńskie

Dokument Polityki Bezpieczeństwa Informacji (PBI)

jest dokumentem zawierającym ogólne zasady i definicje związane z ochroną informacji.

Polityka Bezpieczeństwa Informacji swoim zakresem stosowania obejmuje wszystkie komórki organizacyjne Urzędu Gminy Miasteczko Krajeńskie.

Niniejszy dokument dotyczy wszystkich osób biorących udział, w sposób bezpośredni lub pośredni, w gromadzeniu i przetwarzaniu danych w tym danych osobowych.

POSTANOWIENIA OGÓLNE

§ 1. **Polityka Bezpieczeństwa Przetwarzania Danych Osobowych**, zwana dalej Polityką Bezpieczeństwa została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.) oraz rozporządzenia 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.). Dokument został opracowany zgodnie z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady Europejskiej z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 2. Polityka Bezpieczeństwa określa tryb i zasady ochrony danych osobowych przetwarzanych w **Urzędzie Gminy Miasteczko Krajeńskie**.

§ 3. Ilekroć w Polityce Bezpieczeństwa jest mowa o :

1) **jednostce organizacyjnej** – rozumie się przez to Urząd Gminy Miasteczko Krajeńskie, zwany dalej Urzędem Gminy;
2) **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
3) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

5) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
6) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
7) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
8) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
9) **Administratorze Danych Osobowych** zwanym też **Administratorem Danych (ADO)** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to kierownika jednostki, który decyduje o celach i środkach przetwarzania danych osobowych;
10) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)** - rozumie się przez to osobę wyznaczoną przez Wójta Gminy, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
11) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się przez to osobę zatrudnioną przez kierownika jednostki upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym lub osobę świadczącą usługi informatyczne na rzecz jednostki;
12) **kierowniku komórki organizacyjnej –** rozumie się również samodzielne stanowisko pracy,
13) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez Wójta Gminy, wyznaczonego do

przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył szkolenie prowadzone przez ABI w zakresie ochrony tych danych;

14) **zgodzie osoby, której te dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Rozdział I

CELE

§ 4. Dane osobowe w **Urzędzie Gminy** są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach ,zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych **Urzędu Gminy** na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

§ 5. Polityka bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się swoją treścią do informacji:

1) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
2) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

W systemie informatycznym Urzędu Gminy Miasteczko Krajeńskie przetwarzane są informacje służące do wykonywania zadań z zakresu administracji publicznej i rozwoju instytucjonalnego. Przetwarzane w Urzędzie informacje są między innymi informacjami dotyczącymi :

- informacji publicznych
- danych osobowych
- danych stanowiących tajemnice Urzędu
- innych informacji prawnie chronionych

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

§ 6. Celem opracowania Polityki bezpieczeństwa jest ochrona danych osobowych przed niepowołanym dostępem do zgromadzonych i przetwarzanych danych.

§ 7. Procedury i zasady określone w niniejszej Polityce bezpieczeństwa stosuje się do wszystkich pracowników **Urzędu Gminy**, jak i innych osób mających dostęp do danych osobowych przetwarzanych w **Urzędzie Gminy** (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, wolontariuszy, stażystów, praktykantów, serwisantów).

§ 8.1. Przetwarzanie danych osobowych do celów związanych z działalnością Administratora Danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.

2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, to ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.

3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.

4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji.

§ 9.1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych ustawą należy poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania,
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 10.1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3) źródle danych,
4) prawie dostępu do treści swoich danych oraz ich poprawiania,

5) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
6) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 11. Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują kierownicy komórek organizacyjnych i osoby zatrudnione na samodzielnych stanowiskach.

§ 12.1. Z zasadami w Polityce Bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, składając odpowiednie oświadczenie, którego wzór stanowi załącznik Nr 1 do Polityki Bezpieczeństwa.

2. Oświadczenie wypełnia się w dwóch egzemplarzach; jeden przechowywany jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji ABI.

§ 13.1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy **Urzędu Gminy** oraz osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik Nr 2 do Polityki Bezpieczeństwa. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, właściwych dla komórek organizacyjnych Urzędu*;*

2. Upoważnienie określone w ust. 1 wydawane jest w dwóch egzemplarzach; jeden przechowywany jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji ABI.

2. Ewidencję osób uprawnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji.

3. Wzór ewidencji określonej w ust. 2 stanowi załącznik Nr 3 do Polityki Bezpieczeństwa.

§ 14.1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w jednostce organizacyjnej dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.

2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi.

Rozdział II

ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA OCHRONY PRZETWARZANIA DANYCH

Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych (ADO).

§ 15. Urząd Gminy Miasteczko Krajeńskie korzysta z budynku przy ul. Dąbrowskiego 16. Wejścia do budynku Urzędu Gminy zabezpieczone są zamkami drzwiowymi bezklasowymi oraz systemem alarmowym. Poszczególne pokoje, w których odbywa się przetwarzanie danych i ich składowanie są wyposażone w niezależne zamki, zamykane podczas nieobecności pracownika. Wykaz osób posiadających klucze do pomieszczeń Urzędu Gminy odnotowuje się w *Rejestrze kluczy Urzędu Gminy*, który prowadzi Sekretarz Gminy. Pozostawienie kluczy w zamkach, gdzie przetwarzane są dane osobowe jest niedopuszczalne (także podczas pobytu pracownika w pokoju).

Zabezpieczenie zbiorów przetwarzanych tradycyjnie

1. Zbiory danych przetwarzane tradycyjnie (ręcznie, w kartotekach), po godzinach pracy powinny być przechowywane w szafach zamkniętych na klucz. W przypadku przetwarzania danych, w tym danych osobowych w pomieszczeniu, w którym przebywać

mogą osoby nieupoważnione do przetwarzania takich danych (np. interesanci albo pracownicy) powinny być przeprowadzone w taki sposób, aby osoby nieupoważnione nie miały wglądu do danych.

Zabezpieczenie zbiorów przetwarzanych cyfrowo

1. Stanowiska komputerowe w pomieszczeniach, gdzie przebywać mogą osoby nieupoważnione do przetwarzania danych – w tym danych osobowych (np. interesanci lub inni pracownicy Urzędu), winny być umieszczone w sposób, który uniemożliwi takim osobom wgląd do tych danych.

Na wszystkich komputerach, wymagana jest ochrona antywirusowa. Ponadto te, na których realizowane jest przetwarzanie danych wyposażone powinny być w zasilanie awaryjne umożliwiające bezpieczne zakończenie operacji na danych i zamknięcie systemu – zgodnie z Instrukcją Zarządzania Systemem Informatycznym.

Każdy użytkownik systemu komputerowego korzysta, w celu dostępu do danych, ze stworzonego według określonych zasad konta, o odpowiednich uprawnieniach dostępu do zasobów tegoż systemu do pełnionych obowiązków. Dostęp do konta możliwy jest po podaniu prawidłowej pary – unikalnej nazwy użytkownika i hasła o długości min. 8 znaków i terminie ważności.

W celu zabezpieczenia danych stosowane winny być systemy spełniające odpowiednie normy i zalecenia. Wymaga się, by w miejscu styku sieci komputerowej urzędu z siecią publiczną zastosowane były odpowiednie mechanizmy logiczne lub fizyczne, zapewniające separację zasobów informacyjnych Urzędu Gminy, uniemożliwiające dostęp osób nieupoważnionych z zewnątrz do jej zasobów, a także pozwalające na kontrolę przepływających danych. W systemie wykonywane powinny być kopie zapasowe a ich nośniki przechowywane w bezpiecznym miejscu. Nośniki danych używane w procesie przetwarzania danych, które przestają pełnić swoją funkcję zostają fizycznie zniszczone, będą poddane procesowi „czyszczenia" według określonej procedury uniemożliwiającej ich ponowne odczytanie (szczegółowe wytyczne dotyczące procedur, nośników danych, zabezpieczeń, haseł ich tworzenia i przetwarzania danych osobowych w systemach cyfrowych określone zostały w Instrukcji Zarządzania Systemem Informatycznym).

Przebywanie na terenie Urzędu Gminy Miasteczko Krajeńskie

1. Pracownikom wolno przebywać na terenie Urzędu Gminy tylko w wyznaczonych godzinach pracy, a po nich jedynie po zawiadomieniu i uzyskaniu zgody bezpośredniego przełożonego. Przebywanie w Urzędzie Gminy w dni wolne od pracy możliwe jest jedynie po uzyskaniu zgody Wójta.

Dostęp do zasobów i usług informatycznych

1. Zasoby informatyczne Urzędu Gminy służą do realizowania działań służbowych i nie mogą być wykorzystywane w celach prywatnych.

Dostęp do zasobów i usług informatycznych przydzielany jest wyłącznie na podstawie formalnej ścieżki wnioskowania zdefiniowanej w „procedurze nadawania uprawnień". Zabrania się ingerowania zarówno w sprzęt komputerowy jak i w jego konfiguracjach celem zmiany uprawnień z pominięciem ww. procedury. Przydzielanie dostępu do zasobów i usług informatycznych (w tym podłączanie „obcych" urządzeń do sieci) należących do Urzędu Gminy osobom nie będących pracownikami Urzędu Gminy Miasteczko Krajeńskie, może odbywać się wyłącznie za zgodą Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.

Hasła

Każdy użytkownik , który ma dostęp do systemów informatycznych, posiada unikalną nazwę (login) użytkownika i osobiste hasło.

Użytkownik hasła:

- zobowiązany jest uwierzytelniać się w systemie informatycznym wyłącznie na podstawie własnego loginu i hasła (za wyjątkiem hasła początkowego),
- odpowiedzialny jest za wykorzystywanie swojego loginu i hasła oraz za wszystkie czynności wykonane przy użyciu swojego hasła i loginu,
- w żadnym wypadku nie można ujawniać swojego hasła komukolwiek, włącznie ze służbami informatycznymi, przełożonym czy współpracownikom.

Hasło dostępu nie może być przechowywane w formie możliwej do odczytania, tj. zapisane w plikach tekstem jawnym, skryptach i makrach, w pamięci przeglądarek internetowych, zapisane na kartkach w miejscach, do których mają dostęp osoby nieupoważnione.
Szczegółowe wymogi dotyczące hasła, zasady zabezpieczenia, uzyskania hasła oraz sposób postępowania z hasłem zostały opisane w „Instrukcji Zarządzania Systemem Informatycznym w § 5.

Ochrona przed szkodliwym oprogramowaniem

Na wszystkich stacjach roboczych wykorzystywanych w Urzędzie Gminy zainstalowane jest oprogramowanie antywirusowe. Ingerencja w ustawienia ww. oprogramowania (w szczególności jego wyłączanie lub usuwanie) jest surowo zabroniona.
Każdy pracownik Urzędu Gminy Miasteczko Krajeńskie w przypadku wykrycia szkodliwego oprogramowania na stacji roboczej (lub podejrzenia o zajściu takiego zdarzenia), ma obowiązek bezwzględnie poinformować o tym fakcie Administratora Systemu Informatycznego i postępować zgodnie z otrzymanymi instrukcjami.
Wykorzystywanie jakichkolwiek prywatnych elektronicznych (nośniki optyczne, pendrive, przenośne dyski twarde, itd.) jest zabronione.

Zasada legalności

Użytkowanie na terenie Urzędu Gminy Miasteczko Krajeńskie oraz z wykorzystaniem zasobów Urzędu programów niezgodnie z zasadami licencji jest zabronione. Użytkowanie lub powielanie wszelkich nagrań muzycznych, filmów) oraz innych dzieł podlegających prawom autorskim, nie będących własnością Urzędu Gminy Miasteczko Krajeńskie jest zabronione. Dotyczy to także prywatnych nagrań muzycznych i filmów nabytych legalnie przez pracowników, których używanie na terenie Urzędu lub z użyciem zasobów Urzędu stanowi naruszenie ustawy z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631 ze zm.).
Zawartość stacji roboczych podlega okresowym przeglądom – fakt zidentyfikowania nielegalnych treści zgłaszany jest przełożonym oraz stanowi incydent bezpieczeństwa.

Zasady przekazywania informacji

Wszyscy pracownicy są zobowiązani do zachowania odpowiedniej dbałości o bezpieczeństwo przesyłanych informacji. W szczególności dotyczy to informacji wysyłanych do organizacji i osób spoza struktur Urzędu Gminy.

Przy przesyłaniu informacji przy wykorzystaniu poczty elektronicznej, tradycyjnej, urządzeń faksujących oraz telefonów obowiązują następujące zasady:

- należy przestrzegać drogi służbowej w wysyłaniu korespondencji, jeśli taka została zdefiniowana,
- zabronione jest wykorzystywanie poczty Urzędu Gminy do celów prywatnych i komercyjnych niezwiązanych z realizacją działań służbowych,
- należy upewnić się, że podany został prawidłowy adres odbiorcy informacji,
- należy zapewnić , aby wykorzystywane do przesyłania informacji urządzenie faksujące nie przechowuje treści przesyłki w swojej pamięci,
- nie pozostawia wrażliwych informacji na urządzeniach typu automatyczna sekretarka.

Zasady bezpiecznego użytkowania laptopów

Laptopy podlegają tym samym regułom ochrony jak komputery stacjonarne, ponadto podlegają dodatkowej ochronie prawnej ze względu na traktowanie ich jako baza danych, a szczególnie:

- powinny być zabezpieczone fizycznie podczas użytkowania, transportu oraz przechowywania przed dostępem osób nieuprawnionych i kradzieży (np. specjalna torba, zabezpieczenie przed kradzieżą, nie pozostawianie w widocznym miejscu).
- w trakcie pracy poza terenem kontrolowanym przez Urząd należy zadbać, aby informacje nie były dostępne dla osób postronnych.

Ogólne reguły zabezpieczeń systemu teleinformatycznego

W zakresie ochrony informacji oraz przyjmowania Klientów w Urzędzie Gminy obowiązują następujące zasady bezpiecznej pracy:

- zasada czystego biurka - dokumenty papierowe i nośniki komputerowe, kiedy nie są używane przechowuje się w specjalnych segregatorach, teczkach, szafach, szczególnie poza godzinami pracy, pracownik zobowiązany jest do przechowywania wszystkich dokumentów w szafkach zamykanych na klucz,

- zasada czystego ekranu – w przypadku opuszczania stanowiska pracy, należy zablokować stacje roboczą o mile to możliwe, monitor powinien być ustawiony w taki sposób, aby osoby postronne nie miały możliwości wglądu do przetwarzanych aktualnie informacji, wygaszacze ekranu w stacjach roboczych zostały ustawione na 10 minut,

- zasada odbioru wydruków z drukarki – wszelkie wydruki zawierające dane osobowe klientów, pracowników, informacje o Urzędzie Gminy zabierane są natychmiast z drukarki po zakończeniu drukowania,

- zasada zamykania pomieszczeń – ostatni pracownik opuszczający pomieszczenie zobowiązany jest do zamknięcia okien oraz drzwi zewnętrznych na klucz. Bezwzględnie zakazuje się pozostawiania klucza w zamku po zewnętrznej stronie drzwi,

- zasada poufności rozmów – w przypadku rozmów (również telefonicznych) dotyczących zadań związanych z realizacją zadań Urzędu Gminy, prowadzonych zarówno w siedzibie Urzędu jak i poza obszarem Urzędu, należy zadbać aby rozmowy były prowadzone w obecności osób nieupoważnionych do otrzymania informacji,

- zasada nadzorowania Klientów/gości – Klienci przyjmowani są w pomieszczeniach pracy tylko i wyłącznie pod nadzorem pracowników Urzędu Gminy. Pracownik opiekujący się osobą trzecią zobowiązany jest do nie pozostawiania jej bez nadzoru w przypadku, gdy istnieje możliwość spowodowania przedniego incydentu (np. nieuprawnionego dostępu do informacji).

3. Kierownicy komórek organizacyjnych i samodzielne stanowiska pracy obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w

szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 16. Administrator Danych Osobowych może powołać Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 17.1. Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

2. Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak by wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych i tradycyjnych.

3. Administrator Bezpieczeństwa Informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

4. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji jest następujący:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 1 i 2, oraz przestrzegania zasad w niej określonych,

/administrator danych jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednia do zagrożeń oraz kategorii danych objętych ochroną ,a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą , utratą, uszkodzeniem lub zniszczeniem/.

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (szkolenia);

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7.

3) nadzoruje bezpieczeństwo systemów informatycznych i tradycyjnych;

4) nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących procedur;

5) weryfikuje listę autoryzowanych użytkowników systemów informatycznych;

6) doradza użytkownikom w zakresie bezpieczeństwa;

7) dba, aby użytkownicy mający dostęp do systemu posiadali stosowne upoważnienia oraz byli przeszkoleni w zakresie obowiązujących regulacji bezpieczeństwa;

8) prowadzi kontrolę w zakresie bezpieczeństwa;

9) prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych,

10) przygotowuje wnioski pokontrolne dla Administratora Danych Osobowych,

11) prowadzi rejestr zbiorów danych osobowych przetwarzanych przez administratora danych.

§ 18.1. Administrator Danych Osobowych wyznacza Administratora Systemu Informatycznego (ASI), który posiada najwyższe uprawnienia w systemie informatycznym. Tylko ASI jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.

2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, w taki sposób, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.

3. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Systemu Informatycznego jest następujący:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych i zasobów pamięci systemu, z uprawnieniami administratora,
2) zapewnia stałą sprawność urządzeń mających wpływ na bezpieczeństwo danych;
3) odpowiada za bezpieczeństwo systemu informatycznego;
4) zobowiązuje i na bieżąco kontroluje stosowanie się użytkowników do obowiązujących procedur;
5) utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu informatycznego;
6) zapewnia aktualizację dokumentacji technicznej systemu w tym opis struktur zbiorów i ich zależności;
7) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa informatycznego,
8) przydziela każdemu użytkownikowi danych indywidualne konto w systemie informatycznym Urzędu, stosowne do wyznaczonego przez Administratora Danych Osobowych zakresu obowiązków, na jego polecenie prowadzi ewentualne modyfikacje uprawnień zgodnie z nadaniem ich przez Administratora Danych Osobowych,
9) rejestruje w systemie informatycznym Urzędu poszczególnych użytkowników danych, umożliwiając im dostęp do wyznaczonych kont za pomocą identyfikatorów, a także ich wyrejestrowuje, na polecenie Administratora Danych Osobowych, blokuje ścieżkę dostępu do konta,
10) wprowadza zmiany uprawnień w systemach informatycznych na czas nieobecności pracownika zgodnie z wytycznymi ABI oraz planem zastępstw,
11) prowadzi nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;
12) wykonuje kopie awaryjne/archiwalne /oraz nadzoruje ich przechowywanie;
13) wprowadza i nadzoruje mechanizmy autoryzacji.

§ 19. Kierownik komórki organizacyjnej oraz pracownicy na samodzielnych stanowiskach odpowiadają za przestrzeganie ustawy o ochronie danych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

1) kontrolują sposób zabezpieczenia zbiorów danych osobowych przez pracowników,
2) kontrolują sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie,
3) zgłaszają ABI planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie,
4) wnioskuje o nadanie upoważnień do przetwarzania danych osobowych pracownikom,
5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w **Urzędzie Gminy Miasteczko Krajeńskie.**

§ 20. Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za realizację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

Rozdział III
WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

§ 21. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej w postaci dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).

2. Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych stanowi załącznik Nr 4 do polityki bezpieczeństwa.

§ 22. Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w **Urzędzie Gminy Miasteczko Krajeńskie** wyróżnia się dwie kategorie danych:

1) **dane osobowe zwykłe** - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych.
2) **dane osobowe szczególnie chronione** – zgodnie z art.27 ust.1 ustawy o ochronie danych osobowych (art. 27 ust. 1) wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 23. Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, z uwagi na gromadzone kategorie zbiorów danych osobowych istnieje obowiązek zgłoszenia do rejestracji tych zbiorów Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1i 1a tejże ustawy.

Rozdział V

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

Przetwarzanie i gromadzenie danych osobowych w systemach informatycznych jest dopuszczalne pod warunkiem :

- spełnienia szczegółowych zaleceń dotyczących systemów informatycznych opisanych w niniejszej Polityce,

- posiadania przez systemy informatyczne mechanizmów pozwalających na realizację procesów zabezpieczenia danych oraz danych osobowych opisanych w niniejszej polityce,

Dane osobowe przetwarzane w systemie informatycznym i przesyłane za pośrednictwem sieci informatycznych powinny być zabezpieczone przy użyciu mechanizmów kryptograficznych.

Wszelkiego rodzaju nośniki danych osobowych, które są przekazywane osobom lub podmiotom nieupoważnionym do otrzymania tych danych lub też gdy istnieje podejrzenie, że mogłyby one znaleźć się w rękach osób nie nieupoważnionych do otrzymania danych (np. w procesie likwidacji), pozbawia się danych lub też doprowadza się do stanu uniemożliwiającego ich odczytanie.

Za pozbawienie zapisu odpowiada osoba przekazująca nośnik lub odpowiadająca za realizację zadań, w wyniku, których nośnik może stać się dostępny dla osób nieupoważnionych do otrzymania danych osobowych.

W razie gdy przekazanie nośnika osobie nie będącej pracownikiem Urzędu jest związane z jego naprawą lub konserwacji albo naprawą lub konserwacją urządzenia, dopuszczalne jest pozostawienie zapisanych danych pod warunkiem sprawowania nadzoru przez Administratora Systemu Informatycznego w trakcie trwania naprawy lub konserwacji.

Dane, w tym dane osobowe są zabezpieczane przez tworzenie kopii awaryjnych. Za poprawny przebieg procesu tworzenia kopii awaryjny, jak również za bezpieczne składowanie kopii i ich udostępnianie odpowiada Administrator Systemów Informatycznych. Za składowanie informacji w sposób umożliwiający wykonanie kopii, w szczególności na centralnych serwerach odpowiada ASI.

Za sporządzenie szczegółowych wytycznych w zakresie zabezpieczenia nośników danych osobowych odpowiada ASI.

§ 24.1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki , winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

2. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się w relacji jednostka organizacyjna - mieszkańcy, przedsiębiorcy, kontrahenci, zakład ubezpieczeń społecznych, urząd skarbowy, banki, Narodowy Fundusz Ochrony Zdrowia, urząd wojewódzki, urząd marszałkowski inne jednostki administracji samorządowej i rządowej.

3. Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej **Urzędu Gminy Miasteczko Krajeńskie** sieci zewnętrznych (Plus , Era , Orange , Play, pozostałe sieci komórkowe, WiFi , WiMAX itp.).

Rozdział VI

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 25.1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz Administrator Systemu Informatycznego zapewniający jego prawidłową eksploatację.

2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.

3. W pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe.

4. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

Rozdział VII

UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

§ 26.1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:

1) jakie dane osobowe zawiera zbiór,
2) w jaki sposób zebrano dane,
3) w jakim celu i zakresie dane są przetwarzane,
4) w jakim zakresie oraz komu dane zostały udostępnione.

2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

§ 27.1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane
7) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane

dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych

9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1 - 5, nie częściej niż raz na 6 miesięcy.

§ 28.1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takiej wiadomości ma obowiązek o wystąpieniu osoby, której dane dotyczą, poinformować ABI.

§ 29.1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest kierownik jednostki lub pracownik posiadający wymagane prawem upoważnienie.

2. W przypadku udostępniania danych osobowych w celach innych niż wyłączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 30.1. Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez ADO z uwzględnieniem wymagań określonych w art.31ust.1 tejże ustawy.

Rozdział VIII

ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU

§ 31.1. Użytkownicy systemu zobowiązani są stosować odpowiednie środki bezpieczeństwa w pomieszczeniach, w których zainstalowano sprzęt systemu informatycznego by nie spowodować jego uszkodzenia.

§ 32.1. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

2. Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł. W przypadku, gdy użytkownik zapomni swoje hasło, może on odnowić hasło w porozumieniu z Administratorem Systemu Informatycznego.

Rozdział IX

BEZPIECZEŃSTWO FIZYCZNE

§ 33.1 Dane osobowe, które są przedmiotem przetwarzania zgodnie z przepisami ustawy o ochronie danych osobowych, gromadzone i przechowywane są w serwerach i w postaci tradycyjnej .

2. Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

§ 34.1. Obszar systemów informatycznych w **Urzędzie Gminy Miasteczko Krajeńskie** obejmuje wszystkie pomieszczenia w następującym budynku: budynek Urzędu Gminy przy ul. Dąbrowskiego 16 w Miasteczku Krajeńskim,

§ 35. Pomieszczenia, w których znajdują się systemy informacji winny być:

1) wyposażone w szafy ,meble biurowe zamykane na klucz umożliwiające przechowywanie dokumentów,

2) zamknięte, jeśli nikt w nich nie przebywa.

§ 36. Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą kierownika komórki organizacyjnej, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

Dział X

BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

§ 37. Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

§ 38. Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy kierownika komórki organizacyjnej.

§ 39. Zabrania się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego.

§ 40.1. Dostęp do zbiorów danych osobowych znajdujących się na serwerach następuje po wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.

2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.

3. W przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana, osoba przetwarzająca dane w porozumieniu z ASI powinna dokonać zmiany hasła.

§ 41.1. Elektroniczne bazy danych osobowych są archiwizowane.

2. Kopie są wykonywane na nośnikach magnetycznych.

§ 42. Używanie oprogramowania prywatnego w sieci jest zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

Rozdział XI

KONSERWACJE I NAPRAWY

§ 43. Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

§ 44.1. Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje także jego aktualizację.

2. Za konserwację oprogramowania stanowisk roboczych odpowiedzialny jest kierownik komórki organizacyjnej. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Systemu Informatycznego.

§ 45. Administrator Systemu Informatycznego przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

1) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w pomieszczeniu biurowym znajdującym się w strefie o ograniczonym dostępie;
2) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

Dział XII

PLANY AWARYJNE I ZAPOBIEGAWCZE

§ 46. Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

§ 47. W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na dwa tygodnie. Kopie archiwalne danych są wykonywane na nośnikach magnetooptycznych, i przechowywane są przez Administratora Systemu Informatycznego. Użycie kopii zapasowych następuje na polecenie Administratora Systemu Informatycznego w przypadku odtwarzania systemu po awarii.

Rozdział XIII

POLITYKA ANTYWIRUSOWA

§ 48. 1. Wszystkie serwery i komputery są sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.

2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

1) nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Systemu Informatycznego;
2) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

2. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z administratorem sieci lokalnej.

Rozdział XIV

PRZEPISY KOŃCOWE

§ 49. Za naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

- ***Art.49.1.*** *Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których nie jest uprawniony , podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2;*

  2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

- ***Art. 51. 1.*** *Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

  2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

- ***Art. 52.*** *Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

- ***Art. 53.*** *Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- ***Art. 54.*** *Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- ***Art. 52.*** *Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- ***Art. 53.*** *Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- ***Art. 54.*** *Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

§ 50. W sprawach nie uregulowanych w niniejszej Polityce Bezpieczeństwa Informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, z późn. zm.) oraz rozporządzenia 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).