Załącznik nr 1
Do Zarządzenia nr 25./.2003
Starosty Poznańskiego
Z dnia .22.09.2003r.

Instrukcja ochrony danych osobowych

Starostwo Powiatowe w Poznaniu

STAROSTA POZNAŃSKI
.....
Jan Grabkowski
Starosta

Opracował:

Marek Jóźwiak
Piotr Siwczak

Instrukcja określa:
-zasady postępowania przy przetwarzaniu danych osobowych,
-prawa osób fizycznych, których dane są lub mogą być przetwarza w zbiorach danych.

Rozdział 1
POSTANOWIENIA OGÓLNE

§ 1.

Podstawę prawną do niniejszej instrukcji stanowią:

1. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. Nr 133, poz. 883), zwana dalej "ustawą".
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 roku w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 80, poz. 521), zwane dalej "rozporządzeniem".
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 roku w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. Nr 80, poz. 522).

§ 2.

Ustawa wprowadziła pojęcie „administratora danych„ , którym jest organ, jednostka organizacyjna, podmiot lub osoba fizyczna decydująca o celach i ośrodkach przetwarzania danych osobowych. W przypadku STAROSTWA POWIATOWEGO W POZNANIU administratorem danych jest STAROSTA POZNAŃSKI a z jego upoważnienia - administrator systemu.

Instrukcja określa:

a)zasady postępowania przy przetwarzaniu danych osobowych,

b) prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych.

§ 3.

Dane osobowe mogą być przechowywane:

a) w systemach informatycznych (mogą być nimi również pojedyncze komputery),

b) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych.

§ 4.

Przetwarzanie danych osobowych jest możliwe tylko wtedy, gdy uzasadnia to:

a) dobro publiczne,

b) dobro osoby, której dane dotyczą,

c) dobro osób trzecich,

a dane przetwarza się w zakresie i trybie określonym w ustawie.

§ 5
1. Jednostki i instytucje objęte ochroną danych osobowych to:
a)podmioty publiczne:
-organy państwowe,
-organy samorządu terytorialnego,
-państwowe i komunalne jednostki organizacyjne
-pomioty prywatne, realizujące zadania publiczne, decydujące o celach i środkach przetwarzania danych;
b)podmioty prywatne:

- osoby fizyczne prowadzące działalność gospodarczą,
- spółki prawa handlowego,
- spółki cywilne,
- spółdzielnie,
- fundacje,
- stowarzyszenia,
- kościoły i związki wyznaniowe,

które przetwarzają dane w związku z działalnością zarobków: zawodową lub dla realizacji celów statutowych.

§ 6.
-Instrukcja nie dotyczy osób fizycznych przetwarzając dane wyłącznie do celów osobistych (nie zarobkowych) lub domowych.

Rozdział 2
ZABEZPIECZENIE DANYCH OSOBOWYCH

Obowiązki administratora danych o charakterze formalnym

§ 7.
Administrator danych – Starosta (upoważniona przez niego osoba – administrator systemu), przed przystąpieniem do przetwarzania danych osobowych w systemach informatycznych, jest obowiązany:
1) określić cele, strategię i politykę zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,

2) zidentyfikować i przeanalizować zagrożenia i ryzyko, na które może być narażone przetwarzanie danych osobowych,
3) określić potrzeby w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych, z uwzględnieniem potrzeby kryptograficznej ochrony danych osobowych, szczególnie podczas ich przesyłania za pomocą urządzeń teletransmisji danych,

4) określić zabezpieczenia adekwatne do zagrożeń i ryzyka,

5) monitorować działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych i ich przetwarzania,
6) opracować i wdrożyć program szkolenia w zakresie zabezpieczeń systemu informatycznego

7) wykrywać i właściwie reagować na przypadki naruszenia bezpieczeństwa danych osobowych i systemów informatycznych przetwarzających powyższe dane.

§ 9.

Ponadto administrator danych jest obowiązany do opracowania instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, w szczególności gdy:

a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,

b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 10.

Administrator danych jest zobowiązany do opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji. Instrukcja ta powinna zawierać przede wszystkim:

1) określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnie za te czynności,

2) określenie sposobu rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności,

3) procedury rozpoczęcia i zakończenia pracy,

4) metodę i częstotliwość tworzenia kopii awaryjnych,

5) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,

6) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,

7) sposób dokonywania przeglądów i konserwacji systemu oraz zbioru danych osobowych,

8) sposób postępowania w zakresie komunikacji w sieci komputerowej.

Obowiązki administratora danych o charakterze personalnym

§ 11.

Administrator danych – Starosta wyznacza administratora bezpieczeństwa informacji, czyli osobę odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, a szczególnie za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

§ 12.

Administrator danych może zlecić wykonywanie obowiązków administratora bezpieczeństwa informacji osobie lub podmiotowi nie zatrudnionemu w Starostwie Powiatowym.

§ 13.

W stosunku do każdej osoby zatrudnionej przy przetwarzaniu danych osobowych administrator danych powinien określić zakres odpowiedzialności za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem - w stopniu

odpowiednim do zadań tej osoby przy przetwarzaniu danych.

§ 14.
Każda osoba przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych, a szczególnie z przepisami karnymi wynikającymi z rozdziału ósmego ustawy.

§ 15.
Osoby zatrudnione przy przetwarzaniu danych osobowych, mające do nich dostęp, obowiązane są do zachowania ich w tajemnicy (zarówno w czasie zatrudnienia, jak też po jego ustaniu).

Obowiązki administratora danych o charakterze organizacyjnym

§ 16.
Administrator danych określa pomieszczenia lub części pomieszczenia: tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

§ 17.
Budynek Starostwa lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiając dostęp osób trzecich.

§ 18.
Osoby nieupoważnione mogą przebywać wewnątrz obszaru określonego w § 16 jedynie w obecności osoby zatrudnionej przy przetwarzani tych danych i za zgodą administratora danych lub osoby przez niego upoważnionej.

§ 19

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

Obowiązki administratora danych o charakterze technicznym

§ 20.
Ogólne obowiązki administratora danych w tym zakresie dotyczą:
1) opracowania oraz przekazania procedur związanych z naruszeniem ustawy,
2) określenia procedur, które będą stosowane w celu zabezpieczenia danych,
3) instrukcji dotyczącej zarządzania użytkownikami systemu,
4) procedur logowania i wylogowywania się z systemu,
6) procedur tworzenia kopii zapasowych oraz procedur przechowywania wydruków,
7) instrukcji o komunikacji wewnątrz sieci komputerowej,
8) wskazówek dotyczących utrzymania baz danych oraz bazy danych osobowych.

§ 21

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

§ 22.

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem przetwarzania danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a szczególnie powinna:

a) zabezpieczyć dostęp do komputera hasłem,

b) zabronić używania komputera osobom nie upoważniony i uniemożliwić im dostęp do danych osobowych.

§ 23.

Urządzenia, dyski lub inne informatyczne nośniki, zawierają dane osobowe przeznaczone do:

a) **likwidacji** - pozbawia się wcześniej zapisu tych danych: a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie,
b) **przekazania innemu podmiotowi**, nie uprawnionemu do otrzymania danych osobowych - pozbawia się wcześniej zapisanych danych.
c) **naprawy** - pozbawia się przed naprawą zapisu tych dany(albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 24.

Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytywanie.

§ 25.

Kopie awaryjne należy:

a) przechowywać w innym pomieszczeniu niż przechowywane są zbiory danych osobowych eksploatowane na bieżąco,

b) okresowo sprawdzać pod względem ich dalszej przydatności do odtworzenia danych w razie awarii systemu,

c) bezzwłocznie usuwać po ustaniu ich użyteczności.

§ 26.

Jeżeli istnieją odpowiednie możliwości techniczne, ekrany monitorów stanowisk dostępu do danych osobowych powinny być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.

§ 27.

System informatyczny powinien być wyposażony w mechanizmy uwierzytelnienia użytkownika, a także kontroli dostępu do tych danych, przy czym:

a) za właściwy nadzór nad funkcjonowaniem tych mechanizmów odpowiada administrator bezpieczeństwa informacji,

b) każdy użytkownik systemu informatycznego, w którym przetwarza się dane osobowe, posiada ustalony, odrębny identyfikator i hasło,

c) identyfikator wpisuje się wraz z imieniem i nazwiskiem do ewidencji użytkowników oraz

d) bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła,

e) hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu,
f) identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie,

g) hasła użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie ich ważności,
h) identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z danego systemu informatycznego, unieważnić jej hasło oraz podjąć, inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

§ 28.

Każdej osobie, której dane są przetwarzane w systemie informatycznym, system ten powinien zapewniać odnotowanie:

1) daty pierwszego wprowadzenia danych tej osoby,

2) źródła pochodzenia danych, jeśli dane pochodzić mogą z różnych źródeł,

3) identyfikatora użytkownika wprowadzającego dane,

4) informacji: komu, kiedy, w jakim zakresie dane zostały udostępnione, jeśli przewidziane jest udostępnianie danych inny podmiotom, chyba że dane te traktuje się jako dane powszechnie dostępne,

5) żądania czasowego lub stałego wstrzymania wykorzystywania danych lub ich usunięcia, jeżeli zostały zebrane niezgodnie z prawem lub są już zbędne dla celu ich zebrania.

§ 29.

System informatyczny służący do przetwarzania danych osobowych powinien umożliwić udostępnienie na piśmie, w powszechnie zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, wraz z informacjami wyszczególnionymi w § 28.

Rozdział 3
REJESTRACJA ZBIORÓW DANYCH OSOBOWYCH

§ 30.

Zbiory danych osobowych podlegające rejestracji, powstałe po 30 kwietnia 1998 roku, administrator danych (pełnomocnik ds. ochrony informacji niejawnych) jest obowiązany zgłosić Generalnemu Inspektorowi jeszcze przed rozpoczęciem przetwarzania.

§ 31.

Zgłoszenie zbioru danych osobowych do rejestracji:

a) następuje na formularzu, którego wzór określa rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony, Danych Osobowych (Dz.U Nr 80, poz. 522),

b) powinno zawierać:

- wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych,
- oznaczenie podmiotu prowadzącego zbiór i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadana oraz podstawę prawną upoważniającą do prowadzenia zbioru

- zakres i cel przetwarzania danych,

- sposób zbierania oraz udostępniania danych,

- opis środków technicznych i organizacyjnych zastosowanych w celu zabezpieczenia zbiorów danych osobowych,
- informację o spełnianiu wymagań technicznych i organizacyjnych urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.

§ 32.
Administrator danych nie ma obowiązku rejestrowania (przesyłania) treści zbioru, gdyż sama treść nie podlega rejestracji.

§ 33.
1. Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych:

- objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego,
- przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego,
- dotyczących członków kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej,
- dotyczących osób u nich zatrudnionych, zrzeszonych lub uczących się (także w przeszłości),

- dotyczących osób korzystających z ich usług medycznych (szpitale, przychodnie, ośrodki rehabilitacyjne), obsługi notarialnej,adwokackiej lub radcy prawnego,

- tworzonych na podstawie ordynacji wyborczych do Sejmu, Senatu, rad gmin, ustawy o wyborze Prezydenta Rzeczypospolitej Polskiej oraz ustaw o referendum i ustawy o referendum gminnym,
- dotyczących osób pozbawionych wolności na podstawie ustawy w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,

- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,

- powszechnie dostępnych,

- przetwarzanych w celu przygotowania ,rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

2. Zwolnienie z powyższego obowiązku nie staje się równoznaczne zwolnieniem z innych obowiązków przewidzianych w ustawie (np. obowiązku informacyjnego wynikającego z art. 24 i 25 ustawy).

3. Nie podlegają rejestracji zbiory danych osobowych sporządzonych doraźnie (dla chwilowej potrzeby), a tworzone:

- ze względów technicznych (np. zbiór utworzony tymczasowo który ma służyć utworzeniu większego zbioru danych),

- dla celów szkoleniowych,
- w związku z dydaktyką w szkołach wyższych (zbiory tworzone bezpośrednio dla potrzeb dydaktycznych).

Mają tu zastosowanie jedynie przepisy o zabezpieczeniu zbioru danych osobowych.

§ 34.

Administrator danych osobowych ma obowiązek zgłoszenia Generalnemu Inspektorowi Ochrony Danych Osobowych zmiany obejmując przetwarzanie nowej kategorii danych w terminie do 30 dni od dnia dokonania zmiany w zbiorze danych.

§ 35.

1. Po decyzji o odmowie rejestracji zbioru danych osobowych administrator danych może zgłosić ponownie zbiór do rejestracji po usunięciu wad, które były powodem odmowy rejestracji zbioru.
2. W razie ponownego zgłoszenia zbioru do rejestracji administrator danych może rozpocząć ich przetwarzanie po zarejestrowaniu zbioru.

§ 36.

Inspektor ochrony danych osobowych ma prawo: wstępu w godzinach od 6:00 do 22:00, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zarejestrowany zbiór danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą, żądać złożenia pisemnych lub ustnych wyjaśnień i wzywać oraz przesłuchiwać osoby do ustalenia stanu faktycznego, żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli, żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych, natomiast kierownik kontrolowanej jednostki organizacyjnej lub kontrolowana osoba fizyczna będąca administratorem danych osobowych obowiązane są umożliwić inspektorom ochrony danych wykonanie powyższych czynności.

§ 37.

Obowiązek przewidziany w § 36 nie dotyczy administratorów danych osobowych, które są objęte tajemnicą ze względu na obronność i bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego oraz kościołów i związków wyznaniowych, o uregulowanej sytuacji prawnej, które zbierają dane dotyczące swoich członków.

Rozdział 4
ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

§ 38.

warunków, aby jego działanie dotyczące przetwarzania danych osobowych mogło być uznane za zgodne z prawem:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych (zgoda nie może by domniemana lub dorozumiana z oświadczenia woli o inne treści, lecz wyraźnie dotyczyć przetwarzania danych),

2) zezwalają na to przepisy prawa,

3) jest niezbędne osobie, której dane dotyczą, w celu wywiązanie się z umowy, której jest stroną, lub jest to potrzebne do podjęcia niezbędnych działań przed zawarciem umowy, a osoba zainteresowana wyraziła życzenie, aby w tym celu przetwarzać jej dane osobowe (gdy w wyniku zawarcia umowy jedna ze stron po to, aby ją wykonać, musi wykorzystać informacje dotyczące drugiej strony, np. zawarcie polisy ubezpieczeniowej lub umowy dotyczącej prowadzenia rachunku bankowego),

4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

5) jest niezbędne do wypełnienia usprawiedliwionych celów administratorów danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

§ 39.
Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a spełnienie warunku określonego w § 39 pkt 1 jest niemożliwe, administrator danych może przetwarzać dane bez zgody tej osoby do czasu, gdy uzyskanie zgody będzie możliwe.

§ 40.
Starostwo (administrator danych) ma obowiązek udzielania informacji osobom, których dane przetwarza.
1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, a ustawa nie zezwala na przetwarzanie danych bez ujawnienia faktycznego celu ich zbierania, administrator danych jest obowiązany poinformować tę osobę o:

- adresie swojej siedziby i pełnej nazwie (ewentualnie miejscu swojego zamieszkania oraz imieniu i nazwisku),
- celu zbierania danych, a szczególnie o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

- prawie wglądu do swoich danych oraz ich poprawiania,
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę bezpośrednio po utrwaleniu zebranych danych o:
- adresie swojej siedziby i pełnej nazwie (ewentualnie o miejsc swojego zamieszkania oraz imieniu i nazwisku),
- celu i zakresie (imię, nazwisko, adres, zawód) zbierania danych, a szczególnie o odbiorcach lub kategoriach odbiorców danych

- źródle danych,

- prawie wglądu do swoich danych oraz ich poprawiania,

- prawie żądania zaprzestania przetwarzania danych oraz prawie sprzeciwu.

§ 41.

Przepisu § 41 ust. 2 nie stosuje się, jeżeli:

- przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą (dotyczy służby więziennej lub policji),

- dane przewidziane do zebrania są ogólnie dostępne (np. dane zawarte w książkach telefonicznych),

- dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, nie przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a poinformowanie osób wymagałoby nadmierny, nakładów lub zagrażałoby realizacji celu badania,

- administrator danych nie przetwarza dalej zebranych danych po ich jednorazowym wykorzystaniu.

§ 42.

Na Starostwie (administratorze danych) ciąży również obowiązek ochrony integralności i poprawności przetwarzanych informacji; szczególnie jest on obowiązany:

- przetwarzać je zgodnie z prawem,

- zbierać dla oznaczonych, zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami, gromadzić dane merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

- przechowywać je w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 43.

Starostwo Powiatowe, przetwarzając dane w zbiorach, ma obowiązek udzielenia informacji na wniosek osoby, której dane przetwarza, i przestrzegania jej praw wynikających z ustawy, takich jak:

1) prawo do informacji o:

- **fakcie przetwarzania** przez Starostwo informacji jej dotyczących,
- **pełnym adresie siedziby** Starostwa,
- **celu** przetwarzania danych,
- **zakresie** wykorzystywanych danych (kategorii przetwarzanych informacji),
- **sposobie przetwarzania danych** (np. ręczne przetwarzanie, metody informatyczne, w tym sieć komputerowa itp.),

- **dacie**, kiedy dane zostały włączone do zbioru,

- **treści** danych w zrozumiałej (czytelnej) formie,

odbiorców danych, dającą możliwość skorzystania tej osobie z prawa sprzeciwu,
- **źródle danych** (adres, nazwa lub nazwisko podmiotu lub osoby, od której dane otrzymał). Wyjątek stanowi zachowanie tajemnicy państwowej, służbowej lub zawodowej;
2) prawo żądania uzupełnienia, uaktualnienia i sprostowania danych;
3) prawo żądania czasowego lub stałego wstrzymania przetwarzani danych lub ich usunięcia, jeżeli zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;
4) prawo wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na szczególną sytuację Prawo to nie przysługuje, gdy administrator danych posiada zgody osoby na wykorzystywanie danych, upoważnia go do tego przepis prawa lub gdy przetwarza dane w celu wykonania umowy. Jeżeli administrator nie zamierza uwzględnić wniosku, powinien go przekazać Generalnemu Inspektorowi Ochrony Danych Osobowych;
5) prawo wniesienia sprzeciwu wobec przetwarzania jej danych w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych. Sprzeciw nie dotyczy każdego przetwarzania danych, a jedynie dwóch aspektów:

- sprzeciw można zgłaszać wobec przetwarzania danych dla celów marketingowych i to niezależnie od tego, czy administratorem danych jest firma marketingowa czy podmiot, którego jedynie ubocznym (nie głównym) przedmiotem działalności jest marketing,
- sprzeciw można zgłaszać wobec przetwarzania danych innemu administratorowi danych i to niezależnie od tego, w jakim celu dane zostały zebrane i w jakim są udostępniane.

§ 44.
Na wniosek osoby, której dane dotyczą, Starostwo jest obowiązane, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:

- jakie dane osobowe zawiera zbiór,
- w jaki sposób zebrano dane,
- w jakim celu i zakresie dane są przetwarzane,
- w jakim zakresie oraz komu dane zostały udostępnione.

§ 45.
Na wniosek o podanie informacji złożony przez osobę, której dane dotyczą, Starostwo powinno poinformować tę osobę pisemnie. W pozostałych przypadkach forma udzielania informacji może być różna: telefonicznie, faksem, pocztą elektroniczną lub osobiście,. przy czym ciężar dowodu, iż obowiązek informacyjny spełnił, spoczywa na Starostwie.

§ 46.
Administrator danych (pełnomocnik ds. ochrony informacji niejawnych) odmawia informacji lub udostępnienia danych osobie, której one dotyczą, jeżeli spowodowałoby to:

- **ujawnienie wiadomości stanowiących tajemnicę państwową - zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi, mienia lub bezpieczeństwa porządku publicznego,**

- **zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,**
- **istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.**

Rozdział 5
PRZEKAZYWANIE DANYCH OSOBOWYCH ZA GRANICĘ

§ 47.
Przekazanie danych osobowych za granicę może nastąpić jedynie wtedy, gdy kraj docelowy daje gwarancje ochrony tym danym na swoim terytorium, przynajmniej takie, jak obowiązujące na terytorium RP.

§ 48.
Starostwo ma obowiązek przekazania danych do kraju, który nie daje gwarancji ochrony danym osobowym, ale konieczność ich przesłania wynika z odpowiednich przepisów szczególnych polskiego prawa lub ratyfikowanej umowy międzynarodowej.

§ 49.
W przypadku: braku odpowiednich gwarancji w kraju docelowym, braku przepisu szczególnego oraz postanowienia umowy międzynarodowej Starostwo (administrator danych) może jednak przekazać dane osobowe za granicę, jeżeli zachodzi jedna z poniższych okoliczności:

- osoba, której dane dotyczą, udzieliła na to zgody na piśmie,

- przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie (dotyczy to np. rezerwacji biletu, hotelu za granicą),
- przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem,

- przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych,
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,
- dane są ogólnie dostępne.

Rozdział 6
PRZEPISY KARNE

§ 50.
Określonym obowiązkom wynikającym z Ustawy o ochronie danych osobowych odpowiadają przepisy karne.
1.*(odp. do art.* 23 *ustawy)*
Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne, albo do przetwarzania których nie jest uprawniony
- podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2

1a. *(odp. do art.* 27 *ust.* 1 *ustawy)*

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.

2. *(odp. do art.* 23 *ust.* 1 w *powiązaniu* z *art.* 26 *ust.* 1 *pkt* 2 *i* 4 *ustawy)*
Kto administrując zbiorem danych, przechowuje w zbiorze dane osobowe niezgodnie z celem utworzenia zbioru
- podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
3.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
3a.
Jeżeli sprawca działa nieumyślne
- podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

4.
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.
5.*(odp. do art. 40 i nast. ustawy)*

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych

- podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
6.*(odp. do art.* 24 *i* 25 *i* 32 *ustawy)*

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.

Rozdział 7
UWAGI KOŃCOWE

§ 51.

Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.

Obowiązujące w Polsce regulacje prawne w dziedzinie ochrony danych są zawarte m.in. w Kodeksie cywilnym, Ordynacji podatkowej, Ustawie o Policji, Ustawie o działalności ubezpieczeniowej, Ustawie o statystyce publicznej czy Kodeksie karnym.

STAROSTA POZNAŃSKI
Jan Grabkowski