

Nazwa dokumentu:

POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W PUŁTUSKU

Numer dokumentu:

DS - 46_e-1

	Imię i nazwisko	Stanowisko	Data	Zarządzenie wprowadzające
Opracował:	Grzegorz Rzepkowski	Informatyk, Administrator Bezpieczeństwa Informacji	27.07.2011r.	Zarządzenie Nr 56/2011 Starosty Pułtuskiego z dnia 27.07.2011 r.
Zatwierdził:	Edward Marek Wroniewski	Starosta Pułtuski	27.07.2011r.	

Starostwo Powiatowe w Pułtusk	Nazwa dokumentu: POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W PUŁTUSKU	Data wydania: 27.07. 2011 r.
		Numer dokumentu: DS-46_e-1

SPIS TREŚCI:

ROZDZIAŁ I	Postanowienia ogólne, definicje i objaśnienia
ROZDZIAŁ II	Gromadzenie danych osobowych
ROZDZIAŁ III	Obowiązek informacyjny
ROZDZIAŁ IV	Udzielanie informacji o przetwarzaniu danych osobowych
ROZDZIAŁ V	Rejestracja zbiorów danych osobowych
ROZDZIAŁ VI	Ochrona przetwarzania danych osobowych
ROZDZIAŁ VII	Zasady udostępniania danych osobowych

Załącznik A - Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe.

Załącznik B - Wykaz zbiorów danych osobowych.

Załącznik C - Opis struktury zbiorów danych osobowych przechowywanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi.

Załącznik D - Informacja o przetwarzaniu danych osobowych - *wzór formularza stosowanego dla spełnienia przez Urząd obowiązków wymienionych w §10 ust. 1 i 2 Polityki bezpieczeństwa.*

Załącznik E - Zgoda na przetwarzanie danych osobowych w celach innych niż statutowa działalność Starostwo Powiatowego w Pułtusk - *wzór formularza stosowanego dla spełnienia przez Urząd obowiązków wymienionych w §11 ust. 1 i 2 Polityki bezpieczeństwa.*

Załącznik F - Informacja o zawartości zbioru danych osobowych - *wzór formularza stosowanego dla spełnienia przez Urząd obowiązku wymienionego w §12 ust. 2 Polityki bezpieczeństwa.*

Załącznik G - Upoważnienie/Modyfikacja upoważnienia/Cofnięcie upoważnienia - *wzór wniosku do Administratora Danych Osobowych o upoważnienie imienne do przetwarzania danych osobowych. Wzór imiennego upoważnienia do przetwarzania danych osobowych. Wzór cofnięcia imiennego upoważnienia do przetwarzania danych osobowych.*

Załącznik H - Oświadczenie - *wzór oświadczenia osoby przetwarzającej dane osobowe o zachowaniu w tajemnicy danych z którymi ma styczność oraz stosowanych przy przetwarzaniu danych osobowych środków bezpieczeństwa.*

Załącznik I - Oświadczenie - *wzór oświadczenia o zachowaniu tajemnicy osoby zatrudnionej przy przetwarzaniu danych osobowych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej.*

Załącznik J - Porozumienie w sprawie wykorzystania oddanego do dyspozycji pracownika sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej.

Załącznik 1 – Instrukcja w sprawie trybu postępowania przy przetwarzaniu danych osobowych w Starostwie Powiatowym w Pułtusk

Załącznik 2 – Instrukcja postępowania w przypadku naruszenia bezpieczeństwa danych osobowych

Załącznik 3 – Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektów Starostwa Powiatowego w Pułtusk

Załącznik 4 – Instrukcja zarządzania oprogramowaniem

ROZDZIAŁ I

Postanowienia ogólne, definicje i objaśnienia

§1

1. Polityka Bezpieczeństwa Informacji Starostwie Powiatowym w Pułtuskach jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Starostwo Powiatowe w Pułtuskach z wyłączeniem Systemów „Pojazd” i „Kierowca” (CEPiK) użytkowanych w Wydziale Komunikacji i Dróg, dla których „Instrukcje bezpieczeństwa” zostały opracowane przez PWPW w Warszawie (administratora danych).
2. Podstawą do opracowania i wdrożenia dokumentu są:
 - a) Konstytucja Rzeczypospolitej Polskiej,
 - b) Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (t.j. Dz. U. z 2002 r., nr 101, poz. 926 z późn. zm.),
 - c) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. nr 100, poz. 1024).
3. Polityka Bezpieczeństwa Informacji Starostwa Powiatowego w Pułtuskach zawiera między innymi:
 - a) wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe, stanowiący załącznik A do niniejszej instrukcji;
 - b) wykaz zbiorów danych osobowych przetwarzanych elektronicznie lub w inny sposób, stanowiący załącznik B do niniejszej instrukcji;
 - c) opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi, stanowiący załącznik C do niniejszej instrukcji.
4. Przetwarzanie danych osobowych w Starostwie Powiatowym w Pułtuskach jest dopuszczalne tylko pod warunkiem przestrzegania Ustawy o ochronie danych osobowych (t.j. Dz. U. z 2002 r. nr 101 poz. 926 z późn. zm.) i wydanych na jej podstawie przepisów wykonawczych.

§2

Przez użyte w treści Instrukcji sformułowania należy rozumieć:

1. **Ustawa** - rozumie się przez to Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r., nr 101, poz. 926 z późn. zm.),
2. **Dane osobowe** – rozumie się przez to informacje określone w art. 6 ustawy,
3. **Zbiór danych osobowych** – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
4. **Przetwarzanie danych** – rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, w szczególności gromadzenie, utrwalanie, opracowywanie, zmienianie, usuwanie i udostępnianie,
5. **Administrator Danych Osobowych** – rozumie się przez to osobę funkcyjną decydującą o celach i sposobach przetwarzania danych osobowych oraz o środkach wykorzystywanych przy przetwarzaniu danych osobowych,
6. **Administrator Bezpieczeństwa Informacji** – rozumie się przez to osobę funkcyjną, wyznaczoną przez Administratora Danych Osobowych nadzorującą całokształt zagadnień związanych z ochroną danych osobowych,

7. **Lokalny Administrator Bezpieczeństwa Informacji** – rozumie się przez to osobę funkcyjną, wyznaczoną przez Administratora Danych Osobowych nadzorującą całokształt zagadnień związanych z ochroną danych osobowych w podległym Wydziale,
8. **Administrator Systemu Informatycznego** - rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych odpowiedzialną za funkcjonowanie systemu informatycznego,
9. **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
10. **Osoba zatrudniona przy przetwarzaniu danych osobowych** – rozumie się przez to użytkownika systemu informatycznego, upoważnionego przez Administratora Danych Osobowych do przetwarzania danych osobowych, szczególnie pracownika i każdą inną osobę wykonującą czynności związane z przetwarzaniem danych osobowych w Urzędzie

§3

1. Administrator Danych Osobowych ma obowiązek zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator Danych Osobowych określa zakres przetwarzanych danych osobowych w wydawanych zarządzeniach, regulaminach lub w indywidualnych umowach z podmiotami zewnętrznymi, którym zlecono przetwarzanie danych osobowych.
3. Administrator Danych Osobowych przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach w określonych celach i w określonym zakresie, jeżeli:
 - a) jest to konieczne do realizacji określonych prawem zadań,
 - b) jest to niezbędne do osiągnięcia uzasadnionych celów,
 - c) w innym celu i zakresie, jeśli osoba, której przetwarzane dane dotyczą, wyrazi na to pisemną zgodę.
4. W przypadkach szczególnych cel i zakres przetwarzanych danych mogą określać inne obowiązujące przepisy szczegółowe.

§4

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby wpisane do ewidencji prowadzonej przez Administratora Bezpieczeństwa Informacji.
2. Osoby zatrudnione w Starostwie Powiatowym w Pułtusk przy przetwarzaniu danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.
3. Osoby zatrudnione w Starostwie Powiatowym w Pułtusk przy przetwarzaniu danych osobowych przy wykorzystaniu systemów informatycznych są zobowiązane do postępowania zgodnie z „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji”.

§5

Osoby zatrudnione przy przetwarzaniu danych są zobowiązane powiadomić Administratora Bezpieczeństwa Informacji o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych w każdym zbiorze danych lub systemie. Tryb postępowania określa „Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych”.

§6

W zbiorach danych administrowanych przez Starostwo Powiatowe w Pułtusk zabrania się przetwarzania danych ujawniających:

- a) stan zdrowia
- b) pochodzenie rasowe lub etniczne,
- c) poglądy polityczne,
- d) przekonania religijne lub filozoficzne,
- e) przynależność wyznaniową,
- f) przynależność partyjną lub związkową,
- g) kod genetyczny
- h) nałogi
- i) preferencje seksualne,

chyba, że wymagają tego obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła pisemną zgodę.

§7

Pracownik, który:

1. przetwarza w zbiorze danych:
 - a) dane osobowe, do których przetwarzania nie jest upoważniony,
 - b) dane osobowe, których przetwarzanie jest zabronione,
 - c) dane osobowe niezgodne z celem stworzenia zbioru danych,
2. udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
3. nie zgłasza Lokalnemu Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Bezpieczeństwa Informacji zbiorów danych podlegających rejestracji,
4. nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach,
5. uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw,

podlega odpowiedzialności karnej zgodnie z Ustawą oraz sankcjami zgodnymi z przepisami Kodeksu Pracy.

ROZDZIAŁ II

Gromadzenie danych osobowych

§8

Dane osobowe przetwarzane w Starostwie Powiatowym w Pułtusku mogą być uzyskiwane:

1. Bezpośrednio od osób, których te dane dotyczą.
2. Z innych źródeł, w granicach dozwolonych przepisami prawa.

§9

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe nie mające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

ROZDZIAŁ III

Obowiązek informacyjny

§10

1. Dyrektorzy tych Wydziałów Starostwa Powiatowego w Pułtusk, które zbierają i przetwarzają dane osobowe, są odpowiedzialni za poinformowanie osób, których dane przetwarzają o:
 - a) Adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane.
 - b) Celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
 - c) Prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.
2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy poinformować ponadto o:
 - a) Źródle danych.
 - b) Uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 Ustawy.
3. Wzór formularza stosowanego dla spełnienia przez Starostwo Powiatowe w Pułtusk obowiązków wymienionych w ust. 1 i 2, o ile nie gwarantują spełnienia tego obowiązku inne formularze wypełniane i podpisywane przez zainteresowaną osobę, stanowi załącznik D do niniejszej instrukcji.

§11

1. Materiały dotyczące innej niż ustawowa działalność Starostwa Powiatowego w Pułtusk mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.
2. Kandydaci do pracy w Starostwie Powiatowym w Pułtusk w procesie rekrutacji muszą podpisać pisemną zgodę na przetwarzanie ich danych osobowych lub umieścić i podpisać w składanych dokumentach odpowiednią klauzulę zezwalającą na przetwarzanie swoich danych osobowych.
3. Dokumenty złożone w celu określonym w ust. 2 są przechowywane w komórce organizacyjnej, która przetwarza te dane.
4. Wzór formularza stosowanego dla spełnienia przez Starostwo Powiatowe w Pułtusk obowiązków wymienionych w ust. 1 i 2, stanowi załącznik E do niniejszej instrukcji.

ROZDZIAŁ IV

Udzielanie informacji o przetwarzaniu danych osobowych

§12

1. Osobom, których dane przetwarza się w zbiorze danych Starostwa Powiatowego w Pułtusku, przysługuje zgodnie z Ustawą prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.
2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, musi otrzymać odpowiedź na piśmie w terminie nie przekraczającym 30 dni od daty wpłynięcia wniosku.
3. Informacji tej udziela się na formularzu stanowiącym załącznik F do niniejszej instrukcji.

§13

W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Ustawy, albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

ROZDZIAŁ V

Rejestracja zbiorów danych osobowych

§14

Dyrektorzy Wydziałów (Lokalni Administratorzy Bezpieczeństwa Informacji) Starostwa Powiatowego w Pułtusku, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia Administratorowi Bezpieczeństwa Informacji informacji na temat:

- a) planowanego założenia nowych zbiorów danych osobowych wymagających rejestracji,
- b) wnoszonych zmian do zbiorów już zarejestrowanych,
- c) zgłoszenia zbiorów lub modyfikacji do Generalnego Inspektora Danych Osobowych za porozumieniem Administratora Bezpieczeństwa Informacji.

ROZDZIAŁ VI

Ochrona przetwarzania danych osobowych

§15

1. Administrator Danych Osobowych Starostwa Powiatowego w Puławach zobowiązany jest do wydawania, ewidencjonowania i przechowywania imiennych upoważnień do przetwarzania danych osobowych oraz cofniętych upoważnień. Upoważnienie może zostać wydane na czas określony lub do odwołania. Wydanie cofnięcia upoważnienia jest konieczne wyłącznie w przypadku uprzedniego wydania upoważnienia na czas do odwołania. Wzór formularza upoważnienia i formularza cofnięcia upoważnienia stanowi załącznik G do niniejszej instrukcji.
2. Administrator Danych Osobowych Starostwa Powiatowego w Puławach zobowiązany jest do zbierania, ewidencjonowania i przechowywania:
 - a) oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych z którymi mają styczność oraz stosowanych przy przetwarzaniu danych osobowych środków bezpieczeństwa. Wzór formularza oświadczenia stanowi załącznik H do niniejszej instrukcji.
 - b) oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy. Wzór formularza oświadczenia stanowi załącznik I do niniejszej instrukcji.
 - c) porozumień zawartych z osobami zatrudnionymi przy przetwarzaniu danych osobowych w zakresie wykorzystania oddanego im do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej. Wzór formularza porozumienia stanowi załącznik J do niniejszej instrukcji.
3. Brak ważnego upoważnienia, o którym mowa w punkcie 1, oraz brak podpisanych oświadczeń i porozumienia, o których mowa w punkcie 2, uniemożliwia powierzenie pracownikowi wykonywania zadań i obowiązków związanych z przetwarzaniem danych osobowych.

§16

Administrator Bezpieczeństwa Informacji ma obowiązek zapewnić zapoznanie się osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych.

§17

W celu realizacji powierzonych zadań Administrator Bezpieczeństwa Informacji w Starostwie Powiatowym w Puławach ma prawo:

1. Kontrolować Wydziały w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe.
2. Wydawać polecenia Dyrektorom Wydziałów w zakresie bezpieczeństwa danych osobowych.
3. Informować Administratora Danych Osobowych Starostwa Powiatowego w Puławach o przypadkach naruszenia bezpieczeństwa danych osobowych.
4. Żądać od wszystkich pracowników wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

ROZDZIAŁ VII

Zasady udostępniania danych osobowych

§18

Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§19

1. Zbiory danych udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.
2. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
3. Wniosek jest rozpatrywany przez Lokalnego Administratora Bezpieczeństwa Informacji lub, w przypadku nieobecności Lokalnego Administratora Bezpieczeństwa Informacji, przez osobę zastępującą go, który jednocześnie prowadzi ewidencję wniosków.
4. Decyzję w sprawie udostępnienia danych podejmuje wyłącznie Lokalny Administrator Bezpieczeństwa Informacji lub, w przypadku nieobecności Lokalnego Administratora Bezpieczeństwa Informacji, Administrator Bezpieczeństwa Informacji.

§20

Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli:

1. spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób.
2. dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

§21

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.
2. Podmiot, o którym mowa w ust. 1 jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.
3. Podmiot, o którym mowa w ust. 1 jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie, w jakim reguluje to zawarta umowa.
4. W przypadkach opisanych w ust. 1, 2 i 3, odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na Administratorze Danych Osobowych, co nie wyłącza w żadnym przypadku odpowiedzialności podmiotu, z którym zawarto umowę, z tytułu przetwarzania danych niezgodnie z ustawą.
5. Przy kontroli zgodności przetwarzanych danych przez upoważniony przez Administratora Danych Osobowych podmiot, o którym mowa w ust. 1, stosuje się odpowiednio przepisy art.14 –19 ustawy.